Access Points

AT-WA7500
AT-WA7501

Installation and User's Guide

VERSION 2.3

Allied Telesyn

PN 613-000066 Rev C

Contents

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Preface

This manual provides you with information about the features of the Allied Telesyn AT-WA7500 and AT-WA7501 access points with software release 2.0 (or later). This manual also describes how to install, configure, operate, maintain, and troubleshoot the access points.

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Where to Find Web-based Guides

The installation and user guides for all Allied Telesyn products are available in Portable Document Format (PDF) from on our web site at **www.alliedtelesyn.com**. You can view the documents on-line or download them onto a local workstation or server.

Contacting Allied Telesyn

This section provides Allied Telesyn contact information for technical support as well as sales or corporate information.

Online Support

You can request technical support online by accessing the Allied Telesyn Knowledge Base from the following web site: **www.alliedtelesyn.com/kb**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support & Services section of the Allied Telesyn web site: **www.alliedtelesyn.com**.

Returning Products

Products for return or repair must first be assigned a Return Materials Authorization (RMA) number. A product sent to Allied Telesyn without a RMA number will be returned to the sender at the sender's expense.

To obtain a RMA number, contact Allied Telesyn's Technical Support at our web site: **www.alliedtelesyn.com**.

For Sales or Corporate Information

You can contact Allied Telesyn for sales or corporate information at our web site: **www.alliedtelesyn.com**. To find the contact information for your country, select Contact Us -> Worldwide Contacts.

Management Software Updates

You can download new releases of management software for our managed products from either of the following Internet sites:

- Allied Telesyn web site: **www.alliedtelesyn.com**
- Allied Telesyn FTP server: **ftp://ftp.alliedtelesyn.com**

To download new software from the Allied Telesyn FTP server using your workstation's command prompt, you need FTP client software and you must log in to the server. Enter "anonymous" as the user name and your email address for the password.

Chapter 1

Getting Started

This chapter introduces the Allied Telesyn AT-WA7500 and AT-WA7501 access points, explains their features, and describes how you can use them to expand your data collection network. This chapter covers these topics:

Which Allied Telesyn Access Products Does This Manual Support?

This system manual supports the AT-WA7500 and AT-WA7501 access points with software release 2.2.

Overview of the AT-WA7500 and AT-WA7501 Access Point Products

The Allied Telesyn AT-WA7500 and AT-WA7501 access points deliver reliable and seamless wireless performance to almost any operational environment. They are designed for standards-based connectivity and they support industry standard IEEE 802.11g, 802.11b, and 802.11a wireless technologies.

The AT-WA7500 and AT-WA7501 access points with an IEEE 802.11g radio installed are Wi-Fi certified for interoperability with other 802.11g and 802.11b wireless LAN devices.

The AT-WA7500 and AT-WA7501 access points with an IEEE 802.11g radio installed are Wi-Fi® certified for interoperability with other 802.11b and 802.11g wireless LAN devices.

The AT-WA7500 and AT-WA7501 access points with an IEEE 802.11b radio installed are Wi-Fi certified for interoperability with other 802.11b wireless LAN devices.

The AT-WA7500 and AT-WA7501 access points with an IEEE 802.11a radio installed are Wi-Fi certified for interoperability with other 802.11a wireless LAN devices.

The Allied Telesyn access family consists of these access points:

- AT-WA7500
- AT-WA7501

The access point can be configured as an access point or as a point-to-point or point-to-multipoint bridge. Normally, an access point is connected to a wired local area network (LAN) and provides network access for wireless end devices. A point-to-point bridge connects two wired LANs and is often used to provide wireless communications in locations where running cable is difficult, such as across roads or between buildings. A point-to-multipoint bridge not only connects two wired LANs, but also communicates with wireless end devices.

An access point can also be configured as a wireless access point (WAP) or repeater. A WAP is not connected to a wired LAN; it receives data from wireless end devices and forwards the data to an access point (that is connected to the wired LAN). A WAP is useful in areas that do not support a wired network connection.

On the left, this illustration shows the ways you can manage and configure the access point, and on the right, it shows the access point's general multiport bridge architecture.

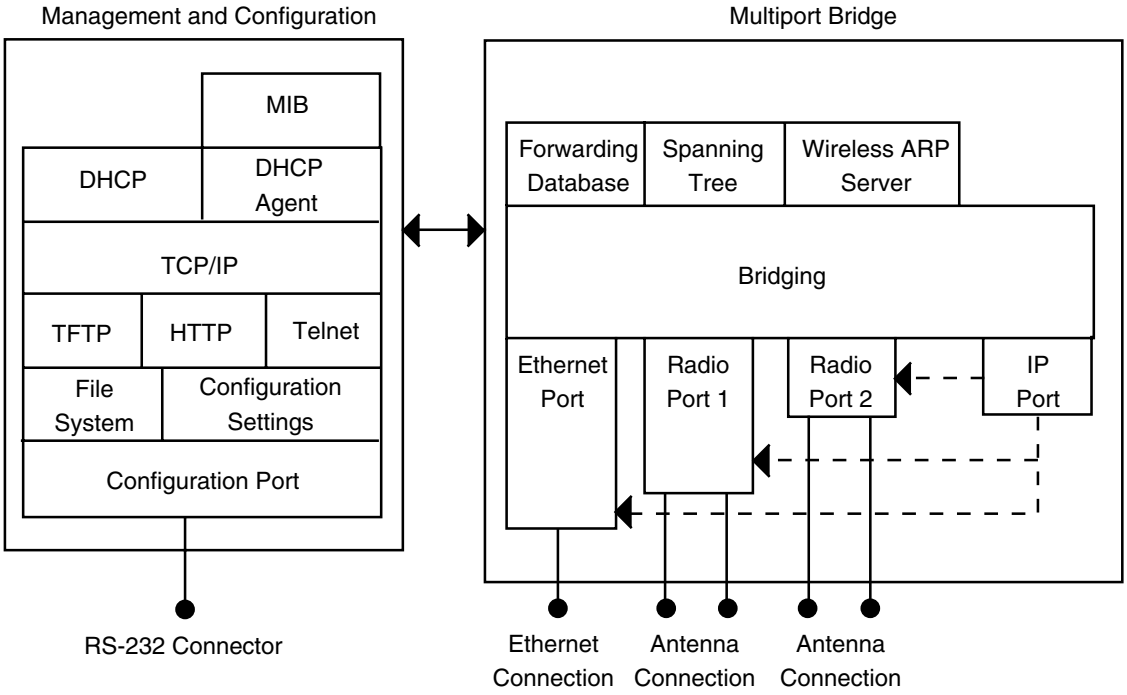


Figure 1. Access Point Architecture

Access points are multiport (Ethernet-to-wireless) bridges, and because wireless end devices operate similarly to other Ethernet devices, all your existing Ethernet applications will work with the wireless network without any special networking software. Any access point, except the root access point, can concurrently receive hello messages on its Ethernet port, its radio port, and its IP tunnel port. However, an access point can use only one port to attach to the network. Port priorities are structured as follows:

1. Ethernet
2. IP tunnel
3. Radio

Unlike the physical Ethernet and radio ports, the IP tunnel port does not have its own output connector. It is a logical port that provides IP encapsulation services for frames that must be routed to reach their destinations. Once frames are encapsulated, they are transmitted or received through the Ethernet or radio port.

Wireless end devices may use power management to maintain battery life. These end devices periodically wake up to receive frames that arrived while their radio was powered down. The access point automatically provides a pending message delivery service that holds frames until the end device is ready to receive them.

Features

This table lists the features of the access points.

Table 1. Access Point Feature Comparison

Feature	AT-WA7500	AT-WA7501
Access Point	Yes	Yes
Point-to-Point Bridge (Wireless Bridge)	Yes	Yes
Wireless Access Point (WAP) or Repeater	Yes	Yes
Secure Wireless Hops (SWAP)	Yes	Yes
Secure Wireless Hops (TLS or TTLS)	Yes	Yes
Radios	802.11g* 802.11b 802.11a	802.11g* 802.11b 802.11a
Dual Radio Support	Yes	Yes
Wi-Fi Compliant	Yes	Yes
Wi-Fi Protected Access (WPA) for 802.1x mode or PSK mode.	Yes	Yes
802.1x Authenticator	Yes	Yes
802.1x Authentication Server	Yes	Yes
Access Control List (ACL) Server	Yes	Yes
Password Server	Yes	Yes
Secure Web Browser Interface (HTTPS)	Yes	Yes
10BaseT/100BaseTx	Yes	Yes
Fiber Optics Option	No	Yes
Serial Port	Yes	Yes
Data Link Tunneling	Yes	Yes
IP Tunneling	Yes	Yes
Antenna Diversity	Yes	Yes
Non-incentive Antenna System	Yes	Yes
NEMA 4/IP 54 Protection	No	Yes
Power Supply	No	AC

Table 1. Access Point Feature Comparison (Continued)

Feature	AT-WA7500	AT-WA7501
Power Over Ethernet	Yes	Yes
Heater Option	No	Yes

* The 802.11g radio is sometimes referred to as the 802.11b/g radio because it can be configured to communicate with any 802.11b and 802.11g radios that have the same SSID and security settings. For details, see “About the Radios” on page 97.

Other features of all access points include:

- the ability to be managed by the Wavelink Avalanche client management system, Allied Telesyn manager, a web browser, telnet, and SNMP.
- the ability to be a DHCP server or client and a NAT server.
- the ability to be an ARP server.
- easy software distribution using the distributed upgrade server.
- advanced filtering of wired data traffic.
- enhanced power management for wireless end devices.
- fast roaming reliability for wireless end devices.
- load balancing.
- basic WEP 64, WEP 128, or WEP 152 security for 802.11g, 802.11b, or 802.11a radios.

What’s New for Software Releases 2.3?

Software release 2.3 can only be installed on the Allied Telesyn AT-WA7500 and AT-WA7501 access points.

Note
To determine the model of your access point, from the menu choose **Maintenance > About this Access Point**. In the **Config String** field, the first five characters tell you the model.

New features include these items:

- **Dual 802.11g radios:** The access points support dual 802.11g radios.
- **Wireless hops and wireless bridging:** The 802.11g radio supports wireless hops and wireless bridging. It also supports WPA security and 802.1x security across the wireless hops.
- **Other new 802.11g radio features:** The 802.11g radio now supports antenna diversity, mixed 802.11g and 802.11b modes, and medium

reservation (including a fragmentation threshold and a reservation threshold).

- **AT-WA7500 Configuration Wizard:** You can use the configuration wizard to help you configure and maintain your access point network.
- **Ability to configure different SSIDs to use different authentication servers.**

Understanding the LEDs

The AT-WA7500 and AT-WA7501 access points have five LEDs. To understand the LEDs during normal use, see the next table. To use the LEDs to help troubleshoot the radios, see "Troubleshooting the Radios" on page 251.

Table 2. LED Descriptions

Icon	LED	Description
	Power	Remains on when power is applied.
	Wireless #1	Blinks when a frame is transmitted or received on the radio port for the radio installed in radio slot 1.
	Wireless #2	Blinks when a frame is transmitted or received on the radio port for the radio installed in radio slot 2 (if a second radio is installed).
	Wired LAN	Blinks when a frame is transmitted or received on the Ethernet port.
	Root/error	Blinks if this device is configured as the root. It remains on if an error is detected.

This illustration shows the LEDs that are on the AT-WA7501 access point. For help understanding these LEDs, see the LED Descriptions table on page 17.

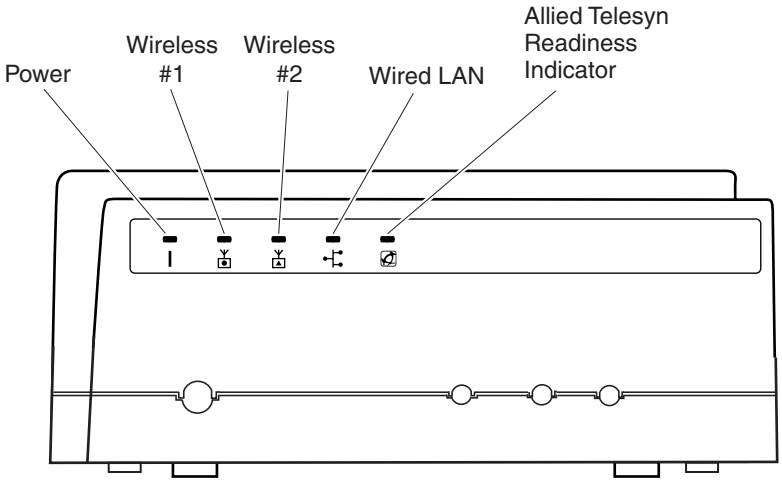


Figure 2. AT-WA7501 LEDs

This illustration shows the LEDs that are on the AT-WA7500 access point. For help understanding these LEDs, see the LED Descriptions table on page 17.

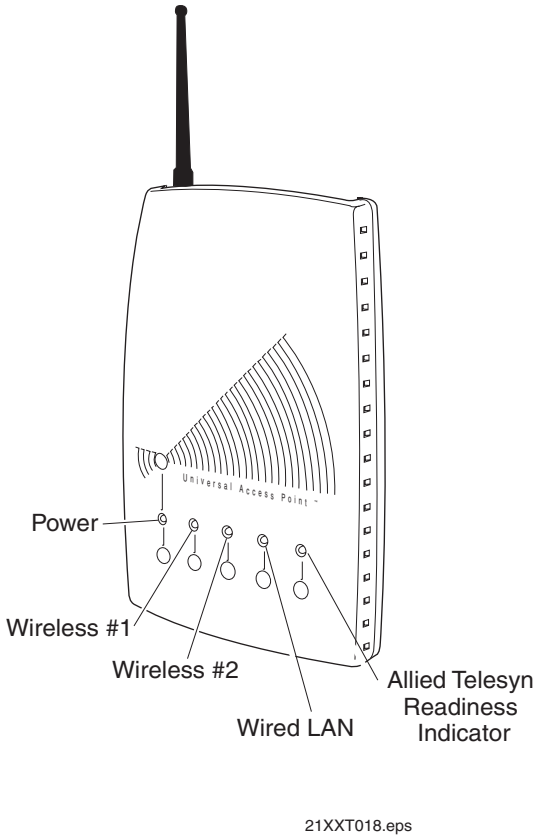


Figure 3. AT-WA7500 LEDs

Understanding the Ports

The access point may have up to four ports.

Table 3. Port Descriptions

Port	Description
Power (Not AT-WA7500, optional AT-WA7501)	Used with an appropriate power cable, this port connects the access point to an AC power source.
Serial	Used with an RS-232 null-modem cable, this port connects the access point to a terminal or PC to perform configuration.
Ethernet	10BaseT/100BaseTx port. Used with an appropriate cable, this port connects the access point to your Ethernet network. The access point auto-negotiates with the device it is communicating with so that the data rate is set at the highest rate at which both devices can communicate.
Fiber optic (Not AT-WA7500, optional AT-WA7501)	Optional 100BaseFX port. You must use a patch cable with a female MT-RJ connector to connect the access point to your MT-RJ, SC, or ST fiber optic network.

To access the ports on the AT-WA7501, you must remove the cable access door.

To remove the AT-WA7501 cable access door

1. Unscrew the two thumbscrews on the cable access door.
2. Remove the door.

This illustration shows the ports that are on the AT-WA7501. For help understanding these ports, see the Port Descriptions table on page 19.

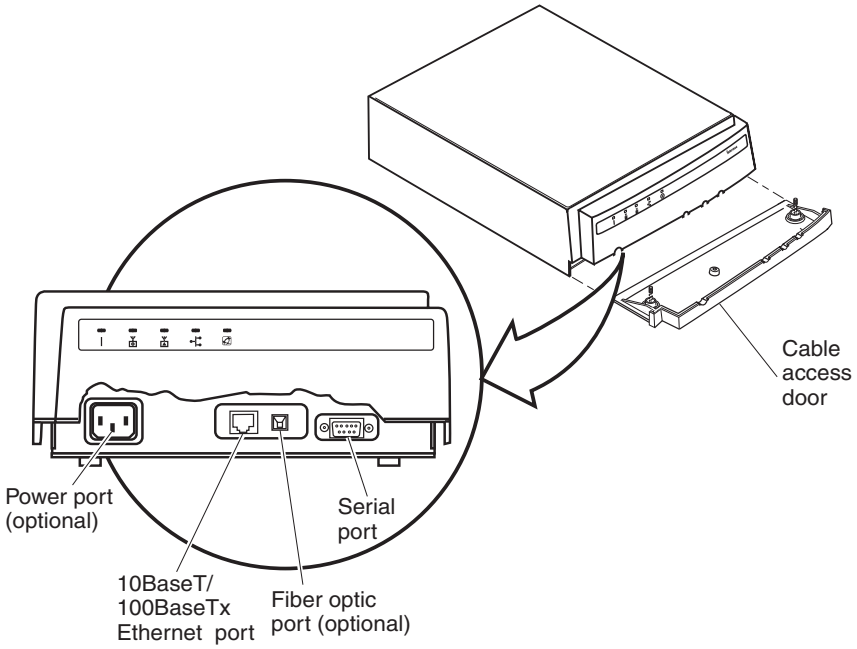


Figure 4. AT-WA7501 Ports

The AT-WA7500 ports are located on the bottom of the access point. This illustration shows the ports that are on the AT-WA7500. For help understanding these ports, see the Port Descriptions table on page 19.

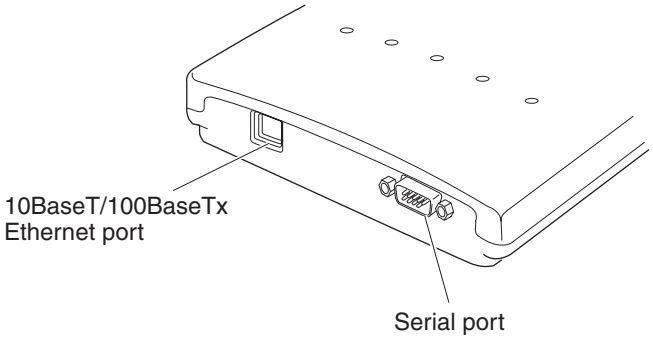


Figure 5. AT-WA7500 Ports

For more information on connecting the ports, see Chapter 2, “Getting Started” on page 11.

How the Access Point Fits in Your Network

In general, the access point forwards data from wireless end devices to the wired Ethernet network. You can also use the access point as a point-to-point bridge, or if your access point has two radios, you can use it as a point-to-multipoint bridge or a WAP. Use the access point in the following locations and environments.

Table 4. Access Point Environments

Access Point	Environment
AT-WA7500	Use in most indoor environments.
AT-WA7501	Use in locations where an access point is exposed to extreme environments.

The access point supports a variety of network configurations. These configurations are explained in the following sections:

- "Using One Access Point in a Simple Wireless Network" on page 21
- "Using Multiple Access Points and Roaming Wireless End Devices" on page 23
- "Using an Access Point as a WAP" on page 25
- "Using Access Points to Create a Point-to-Point Bridge" on page 30
- "Using Dual Radio Access Points for Redundancy" on page 37

Using One Access Point in a Simple Wireless Network

You can use an access point to extend your existing Ethernet network to include wireless end devices. The access point connects directly to your wired network and the end devices provide a wireless extension of the wired LAN.

This illustration shows a simple wireless network with one access point and some wireless end devices.

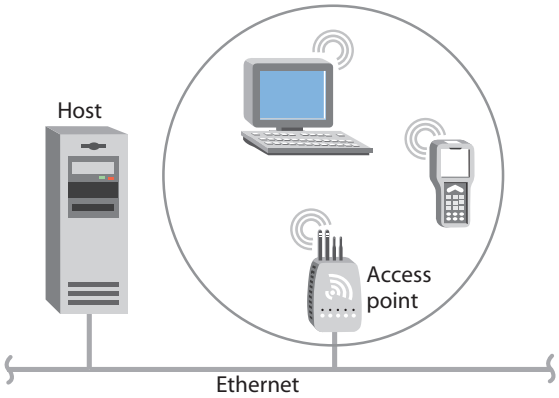


Figure 6. Simple Wireless Network

In a simple wireless network, the access point that is connected to the wired network serves as a transparent bridge between the wired network and wireless end devices.

To install a simple wireless network

1. Configure the initial IP address. For help, see “Configuring the Access Point (Setting the IP Address)” on page 38.
2. Install the access point. For help, see Chapter 2, “Getting Started” on page 11.
3. Configure the Ethernet network. For help, see Chapter 3, “Configuring the Ethernet Network” on page 64.
4. Configure the radios. For help, see Chapter 4, “Configuring the Radios” on page 96.
5. Decide what level of security you want to implement in your network. For help, see Chapter 6, “Configuring Security” on page 169.

Example - Configuring an 802.11g Access Point

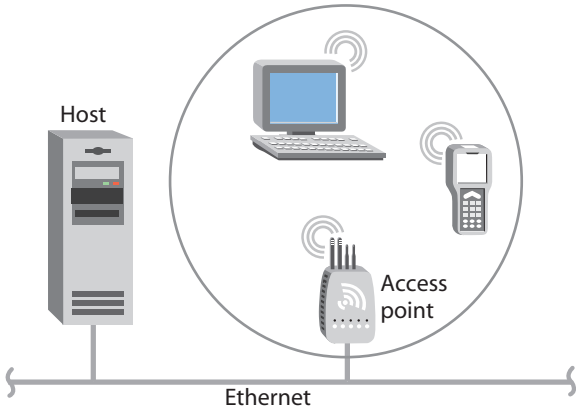


Figure 7. 802.11g Access Point

Table 5. 802.11g Access Point Parameter Settings

Screen	Parameter	Access Point
802.11g Radio	Node Type	Master
	SSID (Network Name)	Manufacturing
Spanning Tree Settings	Root Priority	5
	Ethernet Bridging Enabled	Checked

Allied Telesyn recommends that you always implement some type of security.

Using Multiple Access Points and Roaming Wireless End Devices

For larger or more complex environments, you can install multiple access points so wireless end devices can roam from one access point to another. Multiple access points establish coverage areas or cells similar to those of a cellular telephone network. End devices can connect with any access point that is within range and belongs to the same wireless network.

This illustration shows a wireless network with multiple access points. Wireless end devices can roam between the access points to communicate with the host and other end devices.

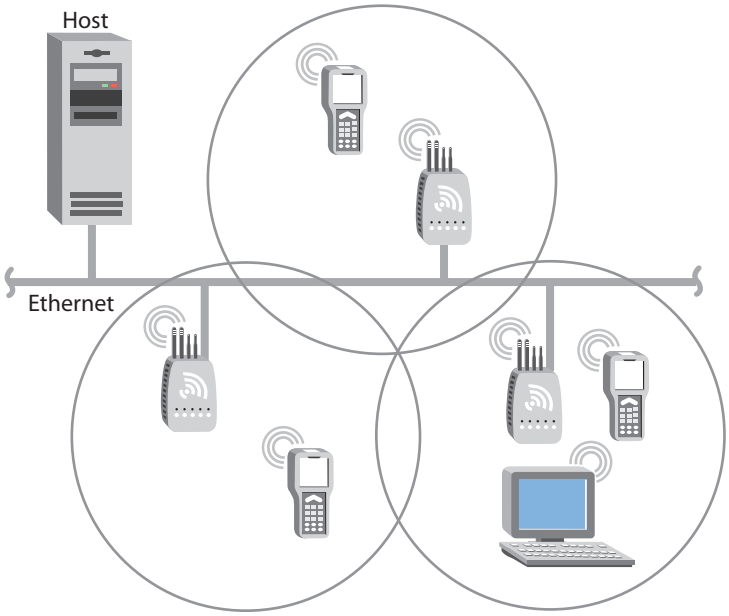


Figure 8. Multiple Access Points with Roaming End Devices

An end device initiates a roam when it attaches to a new access point. The access point sends an attach message to the root access point, which in turn forwards a detach message to the previous access point, allowing each access point to update its forwarding database. Intermediate access points monitor these exchanges and update their forwarding databases.

With the access point's multichannel architecture, you can have more than one access point within the same cell area to increase throughput and provide redundancy. For more information, see "Using Dual Radio Access Points for Redundancy" on page 37.

To install multiple access points with roaming end devices

1. Follow the instructions for installing a simple wireless network in "Using One Access Point in a Simple Wireless Network" on page 21.

2. Configure the LAN ID. For help, see “Configuring the Spanning Tree Parameters” on page 136.

3. Configure one of the access points to be a root access point. For help, see “About the Primary LAN and the Root Access Point” on page 131.

4. If your network has a switch that is not IEEE 802.1d-compliant and is located between access points, configure data link tunneling. For help, see “About Ethernet Bridging/Data Link Tunneling” on page 134.

Example - Configuring an 802.11g Access Point with Roaming End Devices

In this example, there is one 802.11g radio in each access point. Wireless end devices can roam between the access points to communicate with the host and other end devices.

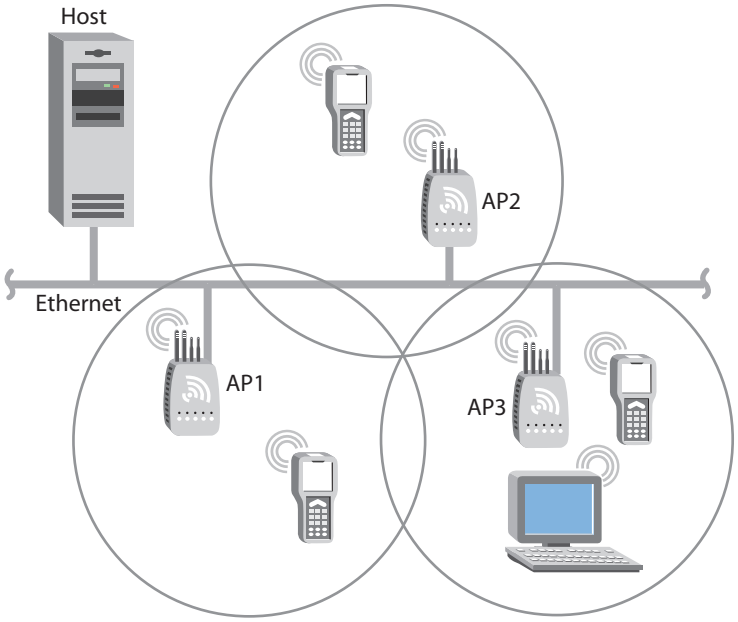


Figure 9. 802.11g Access Point with Roaming End Devices

Table 6. 802.11g Access Points Parameter Settings

Screen	Parameter	AP1 802.11g Radio (Root)	AP2 802.11g Radio	AP3 802.11g Radio
802.11g Radio	Node Type	Master	Master	Master
	SSID	Op3rat!ons	Op3rat!ons	Op3rat!ons
Spanning Tree Settings	LAN ID	0	0	0
	Root Priority	5	4	3
	Ethernet Bridging Enabled	Checked	Checked	Checked
	Secondary LAN Bridge Priority	0	0	0

The access points communicate with each other through the spanning tree. The wireless end devices are configured as stations with LAN ID set to 0 and SSID set to Op3rat!ons.

Using an Access Point as a WAP

You can extend the range of your wireless network by configuring a dual radio access point as a wireless access point (WAP). The WAP and the wireless end devices it communicates with comprise a secondary LAN. You can position WAPs in strategic locations so they receive data from end devices and then forward the data to the wired network. This configuration can be useful when distance or physical layout impedes radio reception and transmission.

This illustration shows a simple wireless network with one access point and one WAP. Wireless end devices use the WAP to forward data to the access point, which forwards data to the host. If you do not want end devices to also be able to communicate directly with the access point, use a different SSID for the access point master radio and the WAP station radio.

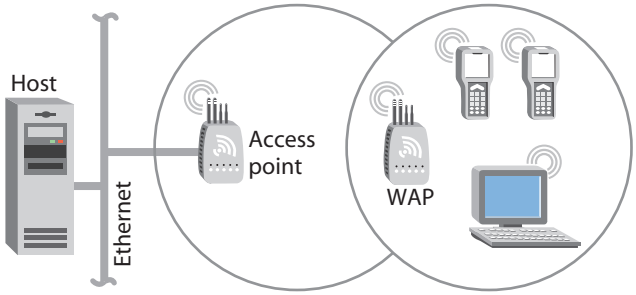


Figure 10. Access Point as a WAP

WAPs send data from end devices to the access points via wireless hops. Wireless hops are formed when data from end devices move from one access point to another access point through the radio ports. The master radio in the access point transmits hello messages, which allow the WAPs to attach to the spanning tree in the same way as access points.

The number of radios required in the WAP depends on the type of radio installed:

- If you have an 802.11a radio, the WAP only needs one radio because this radio can simultaneously be a master and a station. This radio will create wireless hops automatically when it cannot communicate to the wired network.
- If you have an 802.11g or 802.11b radio, the WAP must contain two radios: one configured as master and one as station. The WAP master radio must match the end devices radios, and the WAP station radio must match the master radio in the access point.

WAPs must be on the same IP subnet as the access point. Also, data from wireless end devices should not go through more than three wireless hops before it gets to an access point on the primary LAN.

The following procedure explains how to install a simple wireless network with a WAP and no roaming end devices. For help installing a simple wireless network with a WAP and roaming end devices, see the two examples in the next sections.

To install a simple wireless network with a WAP and no roaming end devices

1. Follow the instructions for installing a simple wireless network in the section “Using One Access Point in a Simple Wireless Network” on page 21.
2. Configure the LAN ID. For help, see “Configuring the Spanning Tree Parameters” on page 136.

3. (802.11g and 802.11b) Configure the station radio in the WAP to communicate with one of the master radio service sets in the access point:

   a. From the main menu, click the link corresponding to the station radio. The radio screen appears.

   b. In the Primary service set Node Type field, choose Station.

   c. In the Primary service set SSID (Network Name) field, type the SSID. In this example, the SSID is Manufacturing.

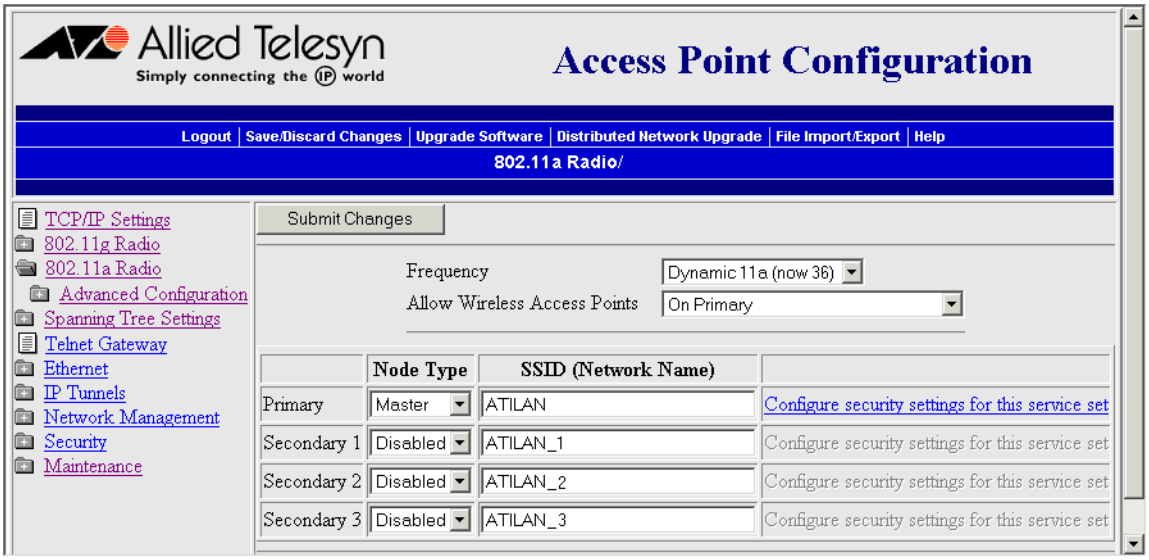
   d. Click Submit Changes to save your changes. The screen updates.

4. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

5. Configure the master radio in the WAP to communicate with the end devices. For help, see Chapter 4, "Configuring the Radios" on page 96.

6. Configure the master radio in the access point:

   a. From the main menu, click the link corresponding to the master radio. The radio screen appears.



   b. In the Frequency field, choose the radio frequency of your wireless network.

   c. (802.11a only) Make sure the Allow Wireless Access Points field is On Primary.

   d. In the Primary service set Node Type field, choose Master.

e. In the Primary service set SSID (Network Name) field, type the SSID that matches the SSID of the end device radio. In this example, the SSID is Manufacturing.

7. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

8. Configure the access point to be a root access point. For help, see “About the Primary LAN and the Root Access Point” on page 131.

9. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

Example - Configuring an 802.11g WAP With No Roaming End Devices

In this example, there is one 802.11g radio in the access point and there are two 802.11g radios (802.11g Radio-1 and 802.11g Radio-2) in the WAP. Wireless end devices only communicate with the WAP; they are not allowed to communicate directly with the access point.

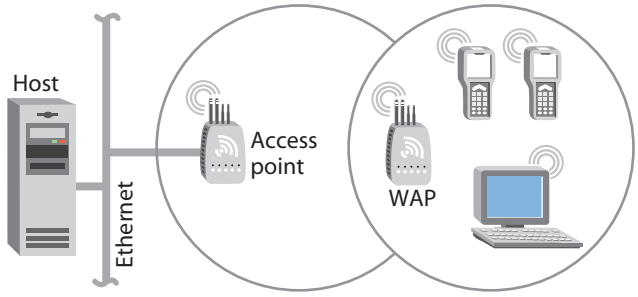


Figure 11. 802.11g WAP with No Roaming End Devices

Table 7. 802.11g Access Point and WAP Parameter Settings

Screen	Parameter	Access Point 802.11g	WAP 802.11g Radio-1	WAP 802.11b Radio-2
802.11g Radio	Node Type	Master	Master	Station
	SSID	Manufacturing	Warehouse	Manufacturing
Spanning Tree Settings	LAN ID	11	11	11
	Root Priority	5	0	(not applicable)
	Ethernet Bridging Enabled	Checked	Checked	(not applicable)

You need to configure the wireless end devices to have the same SSID, LAN ID, and frequency as the WAP radio. You do not need to configure any secondary LAN settings because the WAP is not connected to a secondary LAN.

Allied Telesyn recommends that you always implement some type of security.

Example - Configuring an 802.11a WAP With Roaming End Devices

In this example, there is one 802.11a radio in the access point and there is one 802.11a radio in the WAP. Wireless end devices can roam between the WAP and the access point.

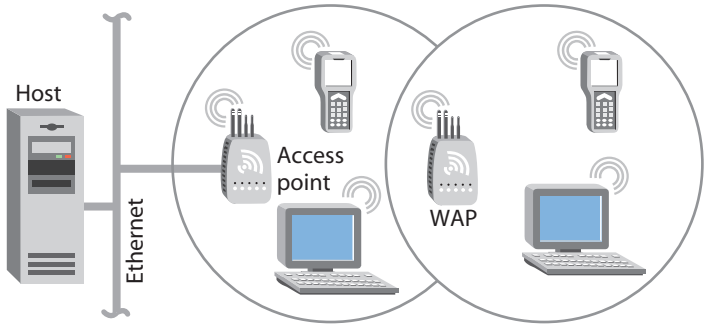


Figure 12. 802.11a WAP with Roaming End Devices

Table 8. 802.11a Access Point and WAP Parameter Settings

Screen	Parameter	Access Point 802.11a	WAP 802.11a
802.11a Radio	Allow Wireless Access Points	On Primary	On Primary
	Primary Node Type	Master	Master
	SSID	Manufacturing	Manufacturing
Spanning Tree Settings	LAN ID	11	11
	Root Priority	5	0
	Ethernet Bridging Enabled	Checked	Checked
	Secondary LAN Bridge Priority	0	0

You need to configure the wireless end devices to have the same SSID, LAN ID, and frequency as the WAP radio. You do not need to configure any secondary LAN settings because the WAP is not connected to a secondary LAN.

Allied Telesyn recommends that you always implement some type of security.

Using Access Points to Create a Point-to-Point Bridge

You can use access points to create a point-to-point bridge between two wired LANs. That is, you can have one access point wired to a primary LAN in one building and have a second access point wired to a secondary LAN in another building. This configuration lets wired and wireless end devices in both buildings communicate with each other, which can be useful in a campus environment or any other environment where pavement or other objects prevent installation of a wired link.

This illustration shows two simple wireless networks that are connected

with access points that are acting as point-to-point bridges.

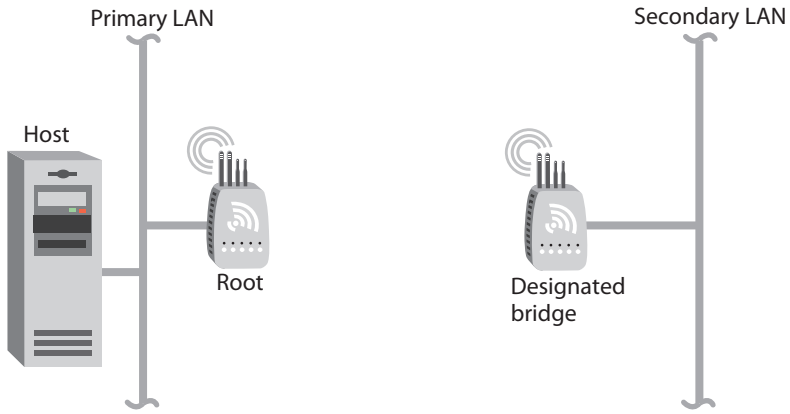


Figure 13. Access Points as Point-to-Point Bridges

Point-to-point bridges send data from end devices on the secondary LAN to the root access point via wireless hops. Wireless hops are formed when data from end devices move from one access point to another access point through the radio ports. The master radio in the point-to-point bridge on the primary LAN transmits hello messages, which allow the bridge on the secondary LAN to attach to the spanning tree in the same way as access points.

How many radios do you need in each access point?

- If you have an 802.11a network, each access point only needs one radio.
- If you have an 802.11g or 802.11b network and the access points are simply acting as point-to-point bridges, each access point only needs one radio.
- If you have an 802.11g or 802.11b network and you want the designated bridge to also communicate with wireless end devices (point-to-multipoint), the designated bridge must have two radios. The designated bridge master radio must match the end device radios, and the station radio must match the root master radio.

Data from wireless end devices should not go through more than three wireless hops before it gets to an access point on the primary LAN.

You need to set the root priorities and secondary LAN bridge priorities for the bridge on the primary LAN and for the bridge on the secondary LAN:

- On the primary LAN bridge, set the root priority to a number that is greater than the root priority of the secondary LAN bridge. The access points will not form a point-to-point bridge if the primary LAN bridge has a lower root priority than the secondary LAN bridge.
- On the secondary LAN bridge, set the root priority to 0 and the secondary LAN bridge priority to a number other than 0.

You may also need to adjust the flooding parameters. Here are some recommendations:

- If there are no end devices on the secondary LAN, the bridge on the secondary LAN can use the default flooding settings. The Secondary LAN Flooding parameter is disabled.
- If there are end devices on the secondary LAN, the bridge on the secondary LAN should have Secondary LAN Flooding parameter set to Multicast. If you also want unicast flooding, you can set this parameter to Enabled.
- If there are end devices on the secondary LAN and the end devices communicate with end devices on another secondary LAN, the root access point should have its Multicast Flooding parameter set to Universal. This setting ensures that all ARP requests and multicast traffic is distributed through a second or third hop.

To install a point-to-point or a point-to-multipoint bridge

1. Follow the instructions for installing a simple wireless network in the section “Using One Access Point in a Simple Wireless Network” on page 21.
2. Configure the LAN ID. For help, see “Configuring the Spanning Tree Parameters” on page 136.
3. Configure one of the master radio service sets in the designated bridge on the secondary LAN to communicate with the end device radios.
4. (802.11g and 802.11b) Configure the station radio in the designated bridge to communicate with one of the master radio service sets in the point-to-point bridge on the primary LAN:
    a. From the main menu, click the link corresponding to the station radio. The radio screen appears.
    b. In the Primary service set Node Type field, choose Station.
    c. In the Primary service set SSID (Network Name) field, type the SSID that matched the SSID of the root access point radio service set (Step 1). In this example, the SSID is Manufacturing.
    d. Click Submit Changes. The screen updates.
5. Configure the spanning tree settings for the designated bridge:
    a. From the main menu, click Spanning Tree Settings. The Spanning Tree Settings screen appears.
    b. In the Root Priority field, enter 0.

c. In the Secondary LAN Bridge Priority field, enter a number other than zero.

d. In the Secondary LAN Flooding field, choose Enabled.

6. Configure the spanning tree settings for the point-to-point bridge on the primary LAN.

   a. From the main menu, click Spanning Tree Settings. The Spanning Tree Settings screen appears.

   b. In the Root Priority field, enter a number other than 0.

   c. In the Secondary LAN Bridge Priority field, enter 0.

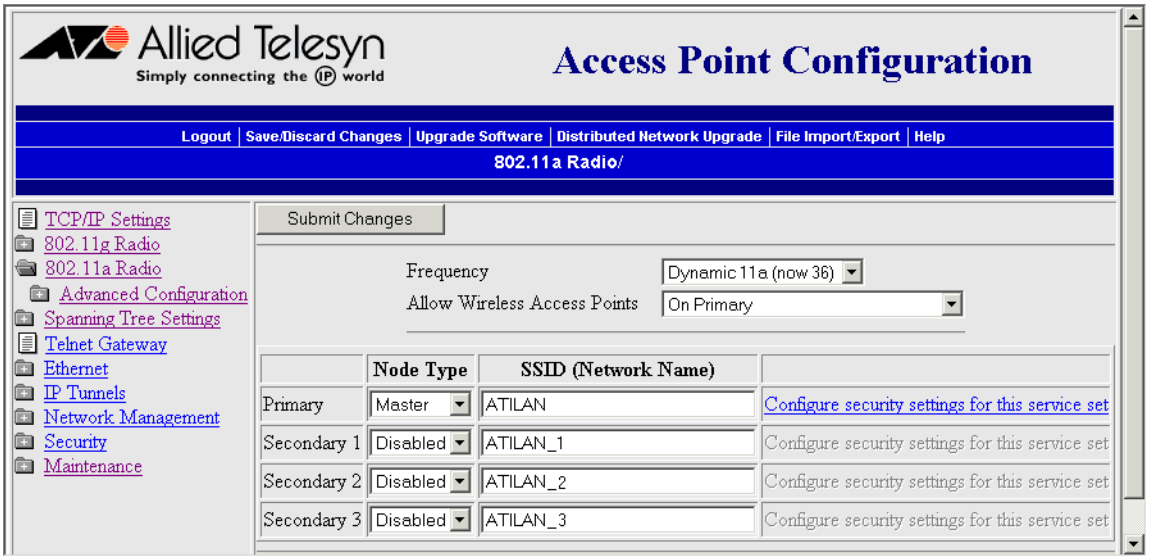
   d. In the Secondary LAN Flooding field, choose Disabled.

7. In the roaming end devices will be roaming across an IP router, you must configure IP tunnels. For help, see "Configuring IP Tunnels" on page 148.

8. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

9. Configure the master radio in the point-to-point bridge on the primary LAN:

   a. From the main menu, click the link corresponding to the master radio. The radio screen appears.



   b. Make sure the Allow Wireless Access Points field is On Primary.

c. In the Primary service set Node Type field, choose Master.

d. In the Primary service set SSID (Network Name) field, type the SSID. In this example, the SSID is Manufacturing.

e. Click Submit Changes.

10. Configure the spanning tree settings for the point-to-point bridge on the primary LAN:

    a. From the main menu, click Spanning Tree Settings. The Spanning Tree Settings screen appears.

    b. In the Root Priority field, enter a number other than 0.

    c. In the Secondary LAN Bridge Priority field, enter 0.

    d. In the Secondary LAN Flooding field, choose Disabled.

11. If the roaming end devices will be roaming across an IP router, you must configure IP tunnels. For help, see “Configuring IP Tunnels” on page 148.

12. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

Example - Configuring an 802.11g Point-to-Point Bridge

In this example, each access point only has one 802.11g radio. Since the designated bridge only has a station radio, wireless end devices can only communicate with the root access point. However, wired devices on the secondary LAN can communicate with the primary LAN.

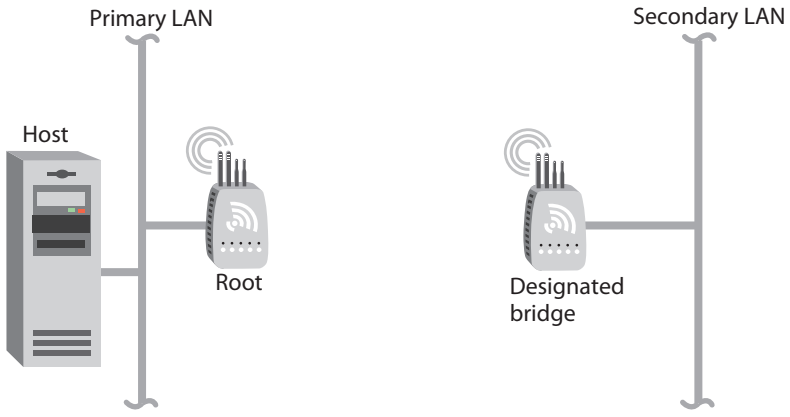


Figure 14. 802.11g Bridge

Table 9. 802.11g Point-to-Point Bridges Parameter Settings

Screen	Parameter	Bridge Primary LAN (Root)	Bridge Secondary LAN (Designated Bridge)
802.11g Radio	Node Type	Master	Station
	SSID	Manufactur-ing	Manufactur-ing
Spanning Tree Settings	LAN ID	0	0
	Root Priority	5	0
	Ethernet Bridging Enabled	Checked	Checked
	Secondary LAN Bridge Priority	0	1
	Secondary LAN Bridge Flooding	Disabled	Enabled

Allied Telesyn recommends that you implement some type of security.

Example - Configuring an 802.11a Point-to-Multipoint Bridge

In this example, each access point only has one 802.11a radio. Since the 802.11a radio can function as a master and a station, wireless end devices can communicate with either access point.

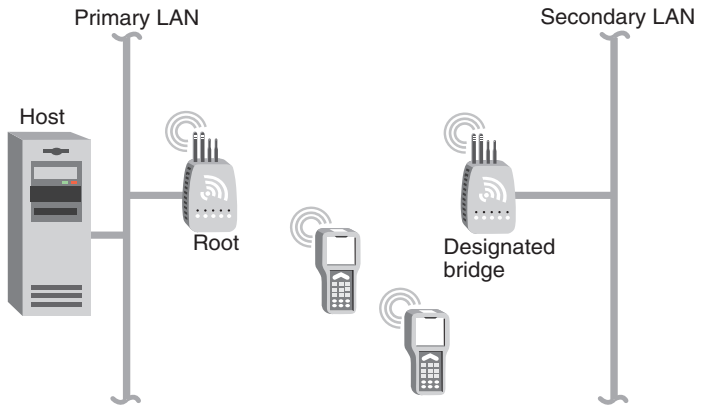


Figure 15. 802.11a Point-to-Point Bridges

Table 10. 802.11a Point-to-Point Bridges Parameter Settings

Screen	Parameter	Bridge Primary LAN (Root)	Bridge Secondary LAN (Designated Bridge)
802.11a Radio	Allow Wireless Access Points	On Primary	On Primary
	Node Type	Master	Master
	SSID	Manufactur-ing	Manufactur-ing
Spanning Tree Settings	LAN ID	11	11
	Root Priority	5	0
	Ethernet Bridging Enabled	Checked	Checked
	Secondary LAN Bridge Priority	0	1
	Secondary LAN Bridge Flooding	Disabled	Enabled

Allied Telesyn recommends that you implement some type of security.

Using Dual Radio Access Points for Redundancy

You can configure AT-WA7500 units and AT-WA7501 units that have two 802.11g radios, two 802.11b radios, or two 802.11a radios to provide redundancy for your network.

During normal operations, end devices send frames to the master radio in one of the access points, which bridges the frames to the wired network. If a section of the wired network goes down, the master radio receives the frames, and then the station radio forwards the frames to a master radio in another access point that is within range.

In each access point, you need to configure one radio's node type as a Master, which communicates with the wireless end devices, and configure the other radio's node type as a Station, which communicates to another access point with a master radio and within range.

In this example, AP3 is a dual radio access point. It may be located on a loading dock or other remote location. During normal operations, AP3 functions as a normal access point, transmitting frames to and from the host. However, if the Ethernet connection is disrupted, AP3 can function as a WAP and continue operations by transmitting frames to a master radio in AP1. AP3 must be within range of AP1.

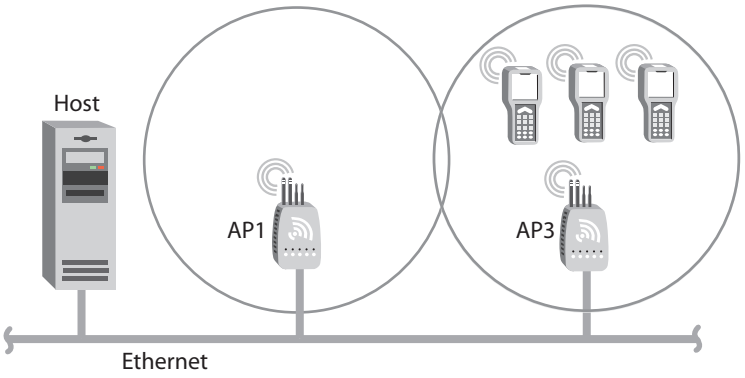


Figure 16. Dual Radio Access Points

To install dual radio access points for redundancy

- ❒ Follow the instructions for installing a simple wireless network with a WAP on page 25.

Configuring the Access Point (Setting the IP Address)

The access point will work out of the box if you are using a DHCP server to assign it an IP address. By default, the access point is configured to be a DHCP client and will respond to offers from any DHCP server. However, if you are not using a DHCP server to assign an IP address, you can use:

- the Allied Telesyn AT-WA7500 Configuration Wizard, but you need to know the access point IP addresses. You can download this wizard from the ATI web site. For help, see “Using the ATI AT-WA7500 Configuration Wizard” on page 38.

  Note
  Your PC must be on the same Ethernet segment as the access point. Or, if your PC is communicating wirelessly with the access point, you must have an active radio connection.

- a communications program, such as HyperTerminal, which also configures other parameters. This program must be installed on a PC with an open serial port. For help, see “Using a Communications Program” on page 40.

This manual assumes that you are using a communications program for your initial configuration, and then using a web browser interface to perform all other configurations. You can also continue to use a communications program or you can start a telnet session to configure the access point.

Using the ATI AT-WA7500 Configuration Wizard

The AT-WA7500 Configuration Wizard is an easy-to-use Microsoft® Windows™-based wizard that lets you:

- set the initial IP address for the access point. This wizard eliminates the need to serially connect a PC to the access point to configure its IP address.
- restore the access point settings to factory defaults. For help, see the only help and “Restoring the Access Point to the Default Configuration” on page 239.
- recover a failed access point. For help, see the online help and “Recovering a Failed Access Point” on page 258.
- upgrade the access point software. For help, see the online help and “Upgrading the Access Points” on page 261.

After you cofigure the IP address, you can use a web browser or a telnet session to complete the configuration.

To use the Allied Telesyn AT-WA7500 Configuration Wizard

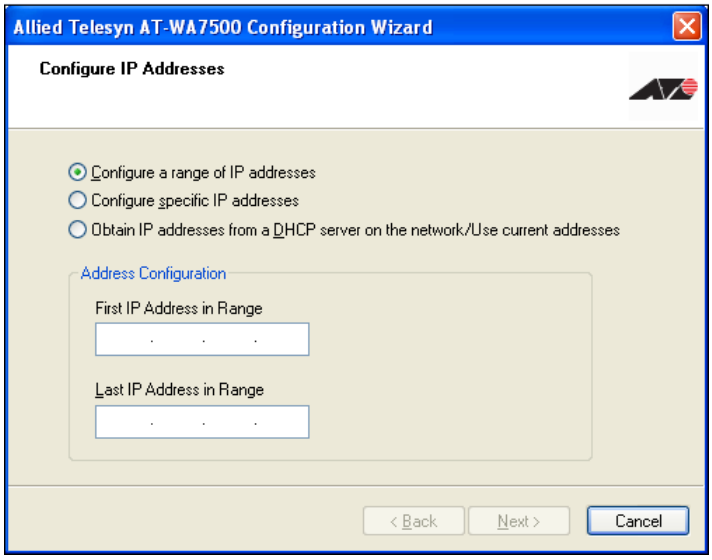
Note
To use the AT-WA7500 Configuration Wizard, you must have a PC that is running Windows 95-OSR2/98SE/ME or Windows NT4/2000/XP.

1. Install the AT-WA7500 Configuration Wizard on your PC. The wizard can be downloaded either from the documentation CD that is shipped with the access point, or from the ATI web site.

2. Extract the .zip file, double-click the .exe file, and then follow the instructions that appear on your screen.

Note
Your PC must be on the same Ethernet segment as the access point. Or, if your PC is communicating wirelessly with the access point, you must have an active radio connection.

3. Start the wizard. The Allied Telesyn AT-WA7500 Configuration Wizard window appears.



4. Select one of the following IP Address configuration options:

   - ❒ Configure a range of IP addresses (default)
   - ❒ Configure specific IP addresses
   - ❒ Obtain IP addresses from a DHCP server on the network/User current addresses

5. Proceed with the IP Address configuration by following the on-screen menus.

Using a Communications Program

You can use a communications program (such as HyperTerminal) to set the initial IP address for the access point. After you configure the IP address, you can continue to use the communications program to set other parameters or you can use a web browser or a telnet session to complete the configuration.

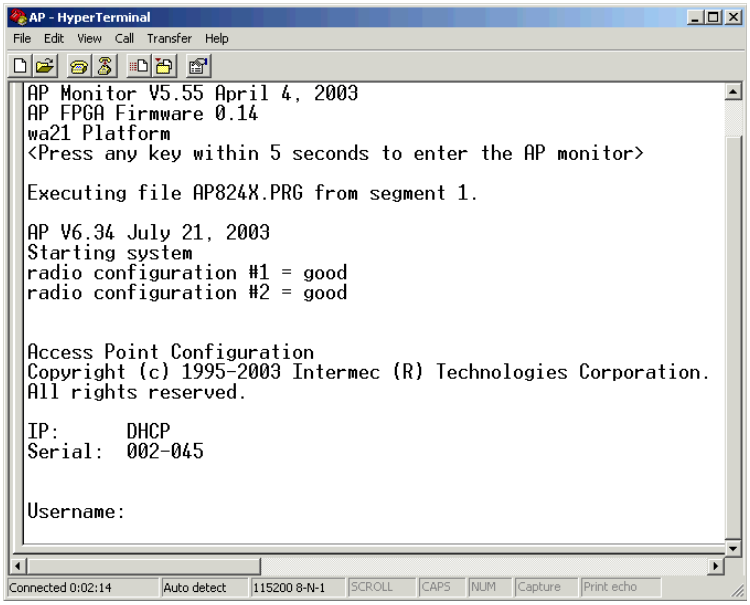
To use a communications program, you must have

- a terminal or PC with an open serial port and the communications program.
- an RS-232 null-modem cable. One end of this cable must be a 9-pin socket connector to connect to the serial port on the access point.

To use a communications program

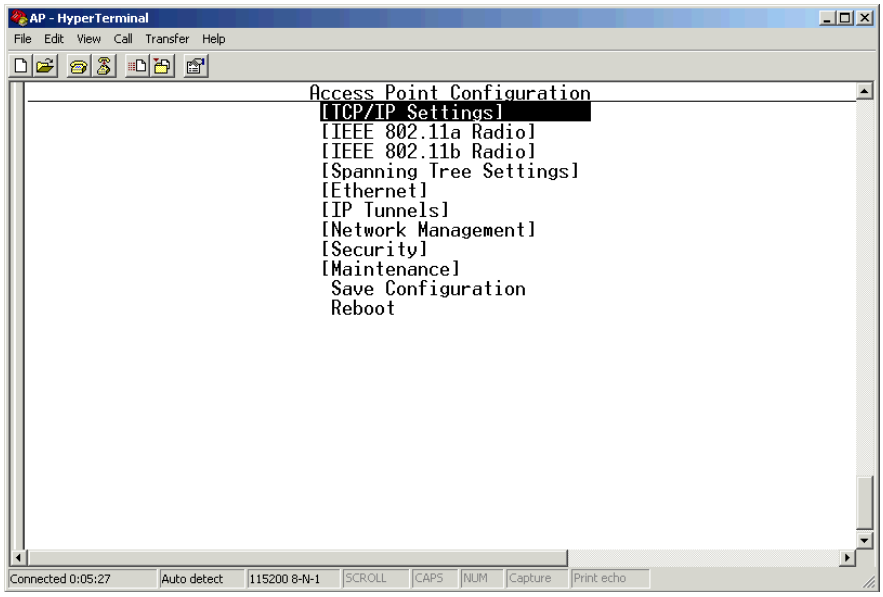
1. Use the RS-232 null-modem cable to connect the serial port on the access point to a serial port on your PC. You may need to remove the serial port plug.
2. Start the communications program and configure the serial port communications parameters on your PC, and then click OK. You should configure the serial port communications parameters to:
   - Bits per second 9600
   - Data bits 8
   - Parity None
   - Stop bit 1
   - Flow control None
3. Connect the access point to power. The access point has no On/Off switch, so it boots as soon as you apply power.

4. Press Enter when the message "Starting system" appears on your PC screen. The Username field appears.



5. In the Username field type the default user name "atilan", and then press Enter. The user name is case sensitive.

6. In the Password field type the default password "atilan", and then press Enter. The password is case sensitive. The Access Point Configuration menu appears.



7. Press Enter to access the TCP/IP Settings menu.

8. If you are not using a DHCP server, you need to manually assign an IP address. Configure these parameters in the TCP/IP Settings menu:

- ❒ IP Address - A unique IP address.
- ❒ IP Subnet Mask - The subnet mask that matches the other devices in your network.
- ❒ IP Router (Gateway) - If the access point will communicate with devices on another subnet, enter the address of the router that will forward frames.

Or, if you are using a DHCP server to automatically assign an IP address to your access point, configure these parameters in the TCP/IP Settings menu:

- ❒ DHCP Mode - Set to <Use DHCP if IP Address is Zero>.
- ❒ DHCP Server Name - The name of the DHCP server that the access point is to access for automatic address assignment. If no server name is specified, the access point responds to offers from any server.

9. Press Esc to return to the Access Point Configuration menu.
10. Choose Save Configuration.
11. Choose Reboot.

When the access point is done rebooting, you are ready to install the access point in your network. See Chapter 2, “Installing the Access Points” on page 49.

Using a Web Browser Interface

After you have set the initial IP address, you can configure, manage, and troubleshoot the access point from a remote location using a web browser interface. The web browser interface has been tested using Internet Explorer. Remotely accessing the access point using other browsers may provide unpredictable results. When using the web browser interface, keep the following points in mind:

- ❒ Your session terminates if you do not use it for 15 minutes.
- ❒ Command Console mode is not available.

Note
If you access the Internet using a proxy server, you must add the IP address of the access point to your Exceptions list. The Exceptions list contains the addresses that you do not want to use with a proxy server.

To use a web browser interface

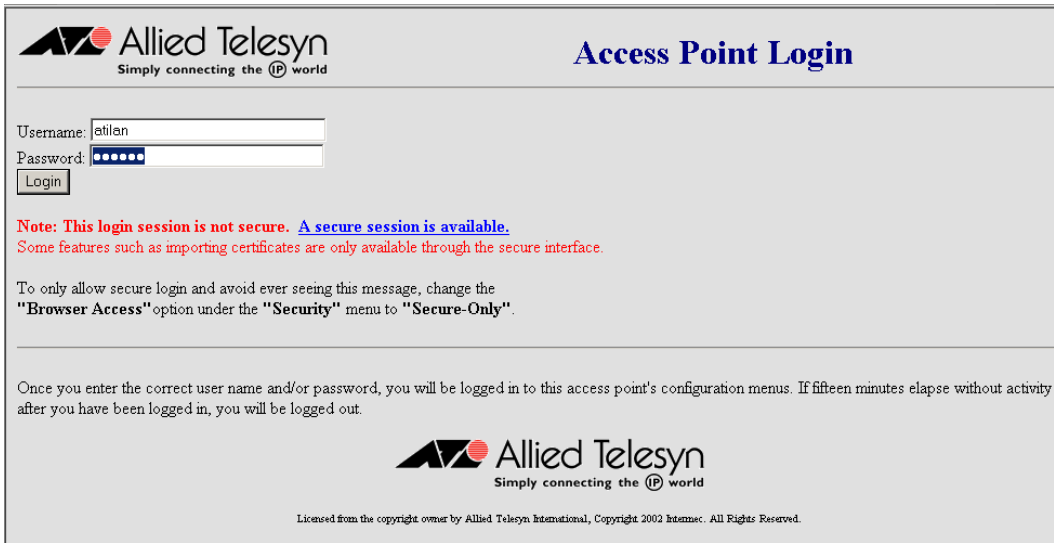
1. Determine the IP address of the access point. If a DHCP server assigned the IP address, you must get the IP address from the DHCP server.

2. Start the web browser application.

3. Access the access point using one of these methods:

   - In the Address field (Internet Explorer) or in the Location field (Netscape Communicator), enter the IP address, and press Enter.
   - From the File menu, choose Open (Internet Explorer) or choose Open Page (Netscape Communicator). In the field, enter the IP address and press Enter.

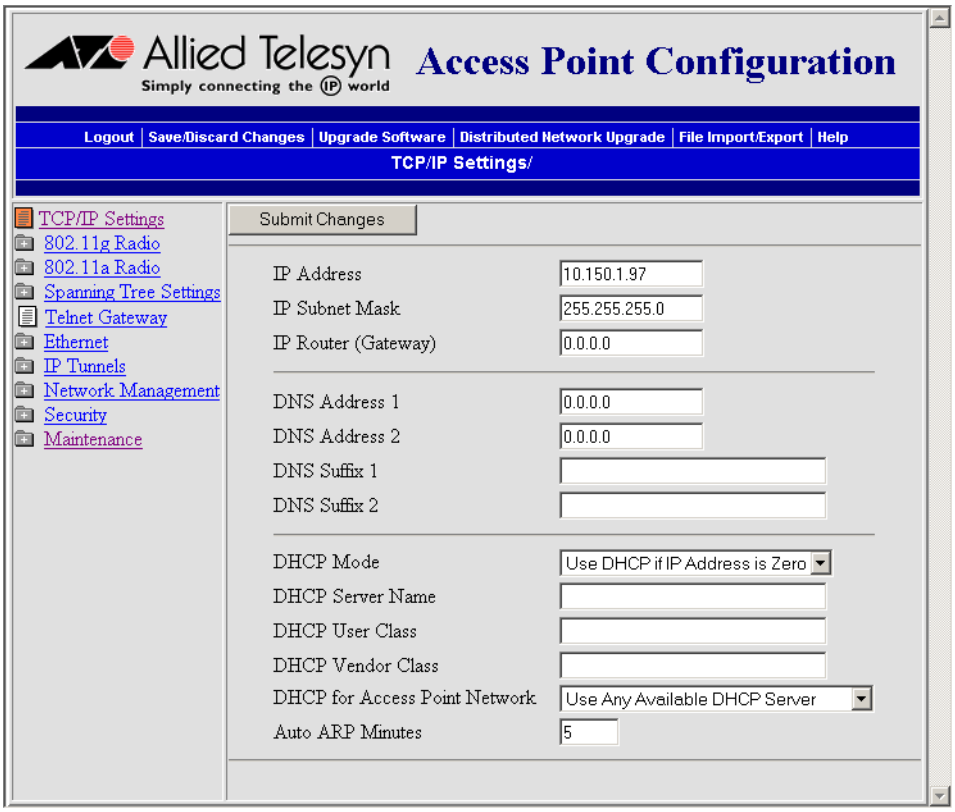
   The Access Point Login screen appears.



4. If necessary, enter a user name and a password. The default user name is "atilan" and the default password is "atilan". You can define a user name and password. For help, see "Setting Up Logins" on page 176.

   Or you may want to log in to a secure session.

5. Click Login. The TCP/IP Settings screen appears.



Your web browser session is established.

Note
Although you can use several different methods to manage the access point remotely, this manual assumes you are using a web browser.

Using a Telnet Session

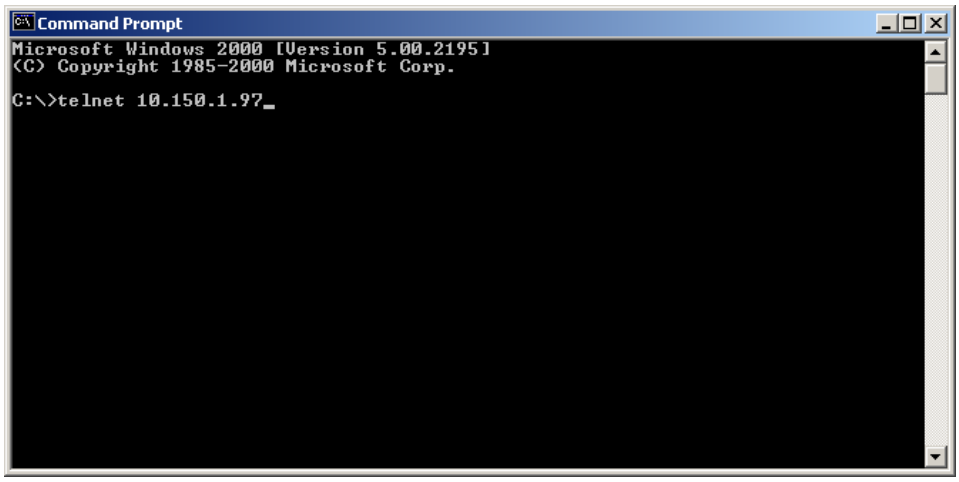
After you have configured the IP address, you can configure, manage, and troubleshoot the access point from a remote location using a telnet session.

Only one session can be active with the access point at a time. If you session terminates abruptly or a new login screen appears, someone else may have accessed the access point. Also, your session terminates if you do not use it for 15 minutes.

To use a telnet session

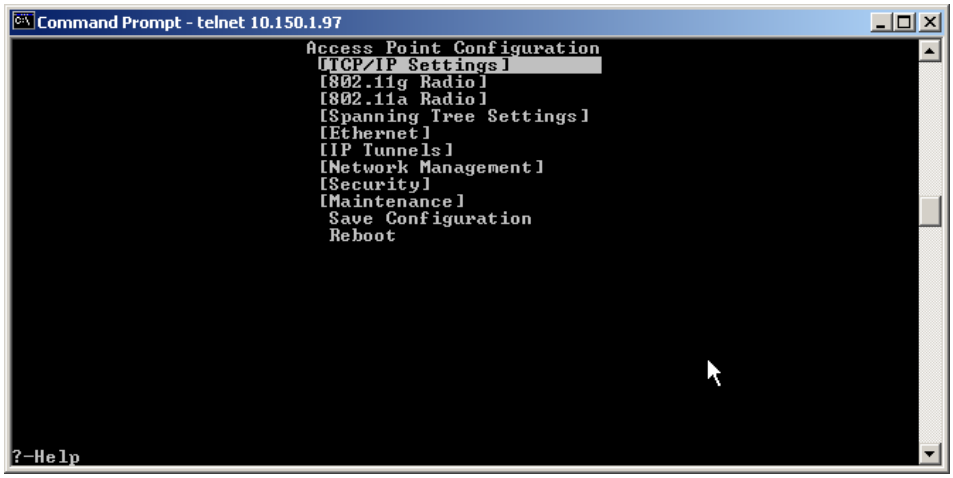
1. Determine the IP address of the access point. If a DHCP server assigned the IP address, you must get the IP address from the DHCP server.

2. From a command prompt, type: **telnet *IPaddress*** where IPaddress is the IP address of the access point.



3. Press Enter.

4. If necessary, enter the user name and press Enter. Then, enter the password and press Enter. The default user name is "atilan" and the default password is "atilan". You can define a user name and password. For help, see "Setting Up Logins" on page 176. The Access Point Configuration menu appears.



Your telnet session is established.

Saving Configuration Changes

When you are done configuring the access point, you may want to activate your changes immediately or you may want to save the changes now and activate them later. If you choose to activate the changes later, they will become active the next time the access point is booted.

Table 11. Access Point Configuration Files

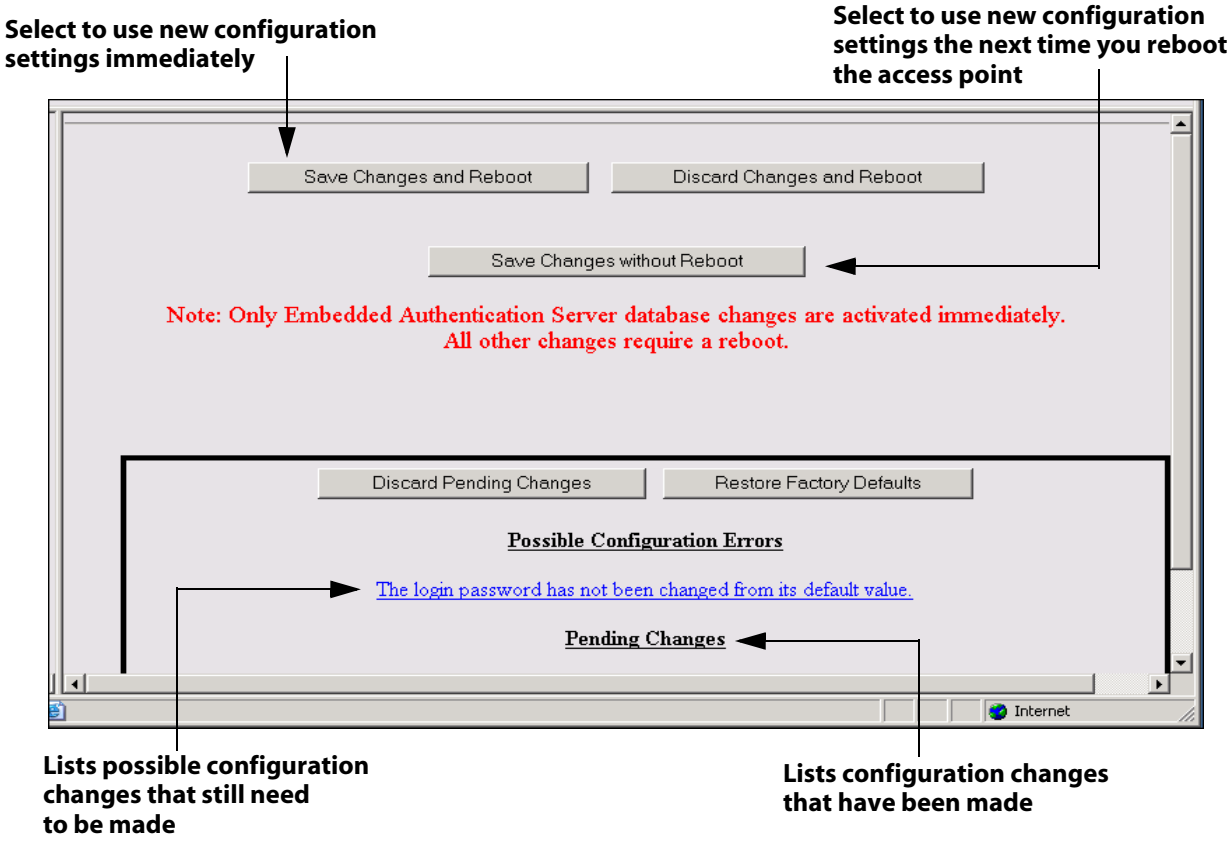
Configuration File	Description
Default	This configuration file is the factory default configuration. For help, see “Restoring the Access Point to the Default Configuration” on page 239.
Current	When you click Submit Changes, the access point updates the current configuration file. The access point does not change the active configuration file. You can see a list of pending changes when you click Save/Discard Changes. Having separate files for the current and active configurations lets you make changes while the access point is running without interrupting communication.
Saved	When you click Save/Discard Changes > Save Changes without Reboot, the access point copies the current configuration file to the saved configuration file. Having separate files for the saved and active configurations lets you make changes while the access point is running without interrupting communication.
Active	When you click Save/Discard Changes > Save Changes and Reboot, the access point copies the current configuration file to the active configuration file. The active configuration file is the file that the access point uses.

Note
For the 802.11g radio, when you configure some of the advanced configuration parameters, you can immediately activate the changes without rebooting the access point. For instructions, see “Applying Hot Settings” on page 108.

Using a Web Browser Interface

1. On the menu bar, click Save/Discard Changes.

This screen appears.



2. Resolve any error messages listed under the heading Possible Configurations Errors. For help, see "Using the Configuration Error Messages" on page 240.

3. Verify that all your configuration changes appear in the Pending Changes box.

4. Click Save Changes and Reboot to reboot the access point and immediately use your new active configuration.

   Or click Save Changes without Reboot. The access point saves the changes to its current configuration and continues to run its active configuration. You need to reboot the access point when you want the current configuration to become the active configuration.

To discard the changes

❒ Click Discard Pending Changes.

Using a Telnet Session

1. From the Access Point Configuration menu, choose Save Configuration.
2. Choose Reboot to reboot the access point and immediately use your new active configuration.

Chapter 2

Installing the Access Points

This chapter explains how to install the Allied Telesyn AT-WA7500 and AT-WA7501 access points in your data collection network, provides some tips on how to position access points to improve your network performance, and provides some external antenna guidelines. This chapter covers these topics:

Installation Guidelines

Allied Telesyn recommends that you have an Allied Telesyn-certified RF specialist conduct a site survey to determine the ideal locations for all your Allied Telesyn wireless network devices. To conduct a proper site survey, you need to have special equipment and training.

The following general practices should be followed in any installation:

- ❒ Locate access points centrally within areas requiring coverage.
- ❒ Overlap access point radio coverage areas to avoid coverage holes.
- ❒ Position the access point so that its LEDs are visible. The LEDs are useful for troubleshooting.
- ❒ Install wired LAN cabling within node limit and cable length limitations.
- ❒ Use an uninterruptible power supply (UPS) when AC power is not reliable.

Proper antenna placement can help improve range. For information about antenna options, contact your local Allied Telesyn representative. For more guidelines, see “External Antenna Placement Guidelines” on page 60.

When determining ideal locations for the access points, be aware that you may see network performance degradation from microwave ovens, cordless telephones, and other access points. For more information, see the next sections.

Note
Microwave ovens, cordless telephones, and other access points do not degrade the network performance of the 802.11a radio.

Microwave Ovens

Microwave ovens operate in the same frequency band as 802.11g and 802.11b radios; therefore, if you use a microwave oven within range of your wireless network, you may notice network performance degradation. Both your microwave oven and your wireless network will continue to function, but you may want to consider relocating your microwave oven out of range of your access point.

Cordless Telephones

If you have an 802.11g or 802.11b radio in your access point, the radio may experience interference from some cordless telephones. For optimal performance, consider operating cordless telephones out of range of your access points.

Other Access Points

Access points that are configured for the same frequency and that are in the same radio coverage area may interfere with each other and decrease throughput. You can reduce the chance of interference by configuring access points at least five channels apart, such as channels 1, 6, and 11.

Installing the AT-WA7501

You can place the AT-WA7501 horizontally or vertically on a desk or counter. If you want to mount the AT-WA7501 to a wall or beam using an Allied Telesyn mounting bracket kit, you need one of these mounting kits:

- ❒ Mounting bracket kit (to be purchased separately)
- ❒ Rotating mounting bracket kit (to be purchased separately)

To order one of these kits, contact your Allied Telesyn representative.

To maintain the IP54 environmental rating, you must mount the AT-WA7501 in either the horizontal or vertical position. If you order the AT-WA7501 with the heater option, you must use one of the mounting bracket kits to mount the AT-WA7501 with the LEDs facing down.

A variety of external antenna options are available for the AT-WA7501. Contact your Allied Telesyn representative for information about the various antenna options, including higher gain and directional antennas. For more information about antennas and antenna accessories, see “Antennas and Antenna Accessories” on page 247.

To install the AT-WA7501, do the following procedure:

1. Attach the antenna or antennas. For more information, see “External Antenna Placement Guidelines” on page 60.

   Note
   If the AT-WA7501 has an 802.11a full-range radio, you must use the antennas that are already attached to the antenna connectors.

2. Mount the AT-WA7501. For help see the AT-WA7501 Quick Install Guide and the instructions that shipped with the bracket kit.
3. Connect the AT-WA7501 to your wired LAN (unless you are using it as a WAP). For help, see “Connecting the AT-WA7501 to Your Wired LAN” on page 52.
4. Connect the AT-WA7501 to power. For help, see “Connecting the AT-WA7501 to Power” on page 53.

   When you are done installing the access points, you need to configure them to communicate with your network.

Connecting the AT-WA7501 to Your Wired LAN

Unless you are using the AT-WA7501 as a WAP, you need to connect it to your Ethernet or fiber optic network. To connect the AT-WA7501 to your fiber optic network, you must have a AT-WA7501 with the fiber optic

option. For help, see "Connecting to Your Fiber Optic Network" on page 55.

To connect the AT-WA7501 to the Ethernet network

- ❒ Attach one end of the Ethernet cable to the 10BaseT/100BaseTx port on the AT-WA7501 and attach the other end to your Ethernet network or a power bridge (if you are using power over Ethernet), a Cisco power bridge or another 802.3af-compliant power bridge.

Connecting the AT-WA7501 to Power

If your AT-WA7501 has the internal power supply option, you can use a power cord to connect the AT-WA7501 directly to an AC power outlet.

Caution

You must use the appropriate Allied Telesyn power supply with these devices or equipment damage may occur.

Attention: Vous devez utiliser la source d'alimentation Allied Telesyn adéquate avec cet appareil sinon vous risquez d'endommager l'équipement.

If you are using the power over Ethernet option, you must have the power bridge or another 802.3af-compliant power bridge. For help, see "Connecting Power Over Ethernet" on page 59 and the documentation that came with your power bridge.

To connect the AT-WA7501 to power

- ❒ Plug one end of the power cord into the power port on the AT-WA7501 and plug the other end into an AC power outlet. The access point boots as soon as you apply power.

Installing the AT-WA7500

You can place the AT-WA7500 horizontally on a desk or counter. The AT-WA7500 also ships with a mounting bracket that lets you mount it vertically to a wall. Additional mounting options that you can use with the mounting bracket include a cubicle bracket that lets you mount the AT-WA7500 on a cubicle wall or in a locking bracket.

- Cubicle bracket kit
- Locking bracket kit

To order one of these kits, contact your Allied Telesyn representative. Allied Telesyn also offers a variety of antennas and antenna accessories. For more information, see “Antennas and Antenna Accessories” on page 247.

To install the AT-WA7500, do the following:

1. Attach the antenna or antennas. For more information, see “External Antenna Placement Guidelines” on page 60.

   Note
   If the AT-WA7500 has an 802.11a full-range radio, you must use the antennas that are already attached to the antenna connectors.

2. Mount the AT-WA7500. For help see the AT-WA7500 Quick Install Guide and the instructions that shipped with the bracket kit.
3. Connect the AT-WA7500 to your wired LAN (unless you are using it as a WAP). For help, see “Connecting the AT-WA7500 to Your Wired LAN and Power” on page 54.
4. Connect the AT-WA7500 to power. For help, see “Connecting the AT-WA7500 to Your Wired LAN and Power” on page 54.

When you are done installing the access points, you need to configure them to communicate with your network.

Connecting the AT-WA7500 to Your Wired LAN and Power

Unless you are using the AT-WA7500 as a WAP, you must connect it to your Ethernet network. To connect the AT-WA7500 to your Ethernet network and to power, you must first connect it to a power bridge or another 802.3af-power bridge. For help, see “Connecting Power Over Ethernet” on page 59 and the documentation that shipped with your power bridge.

Connecting to Your Fiber Optic Network

You can order your AT-WA7501 access point with a fiber optic option. Using an appropriate patch cord and adapter (as described in the next section), you can connect your access point to:

- an MT-RJ network.
- a square connector (SC) network.
- a straight tip (ST) network.

Using and Purchasing the Required Patch Cord and Adapter

To connect the access point with the fiber optic option to your fiber optic network, you must have a patch cord and an adapter.

The access point fiber optic port consists of a male MT-RJ connector interface. Therefore, the patch cord must have a female MT-RJ connector that you insert into the access point fiber optic port.

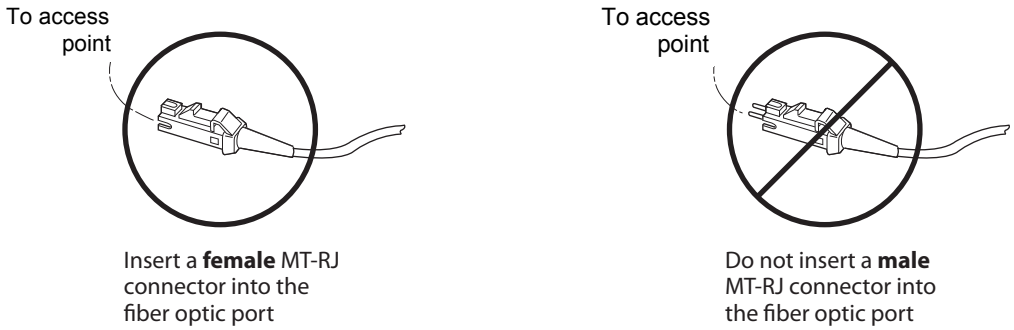


Figure 17. Patch Cord

Note
Inserting a male MT-RJ connector into the fiber optic port may result in unreliable operation because there is no internal mechanism to ensure the alignment of the fiber when using male-to-male connectors. Such a connection may temporarily provide some level of connectivity, despite a high level of signal loss. However, any movement of the cable or change in cable tension could cause complete loss of signal.

Both the connector at the other end of the patch cord and the adapter you select depend on the type of network to which the access point is connected: MT-RJ, SC, or ST.

Patch cords and adapters are available from many different manufacturers. For help choosing the proper patch cord and adapter, contact your local Allied Telesyn representative.

Note
All cables must be multimode, 62.5/125 µm.

Connecting to an MT-RJ Network

To connect to an MT-RJ network, you need:

- a patch cord with a female MT-RJ connector to insert into the access point's male MT-RJ fiber optic port, and another female MT-RJ connector to insert into the MT-RJ adapter.
- an adapter for connecting the patch cord to the MT-RJ network.

To connect to an MT-RJ network

1. Remove any cable protectors attached to the patch cord and adapter.
2. Connect the access point to your network as shown in the next illustration.

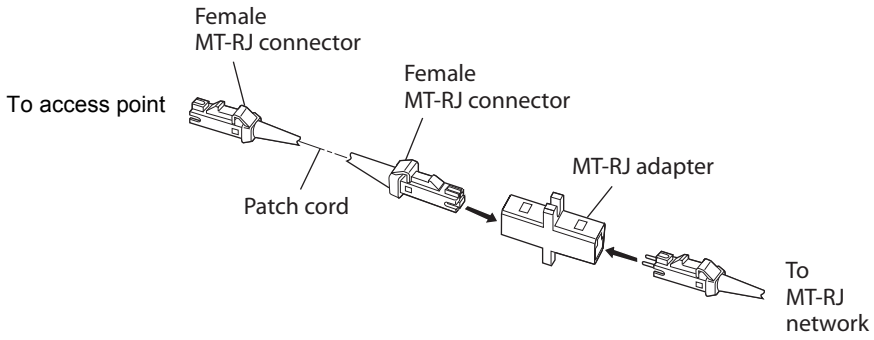


Figure 18. Connecting to an MT-RJ Network

Note
The patch cord shown above must connect to the access point with a female MT-RJ connector. For details, see "Using and Purchasing the Required Patch Cord and Adapter" on page 55.

Connecting to an SC Network

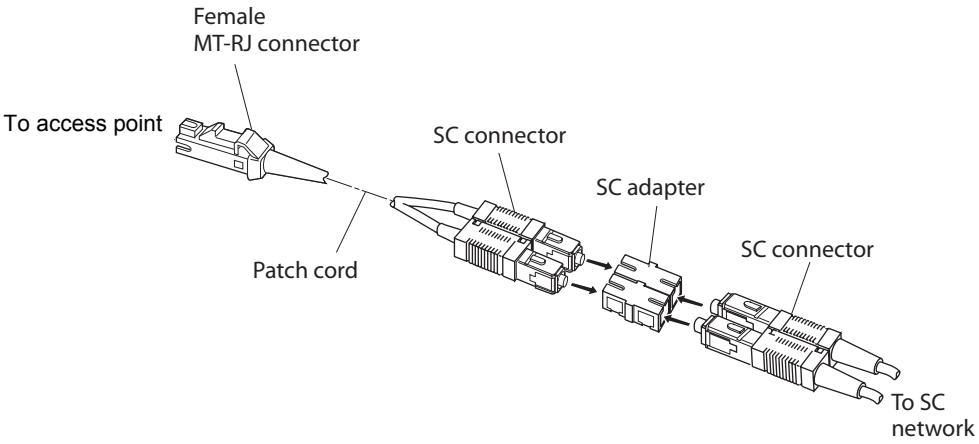
To connect to an SC network, you need:

- a patch cord with a female MT-RJ connector to insert into the access point's male MT-RJ fiber optic port, and an SC connector to insert into the SC adapter.
- an adapter for connecting the patch cord to an SC network.

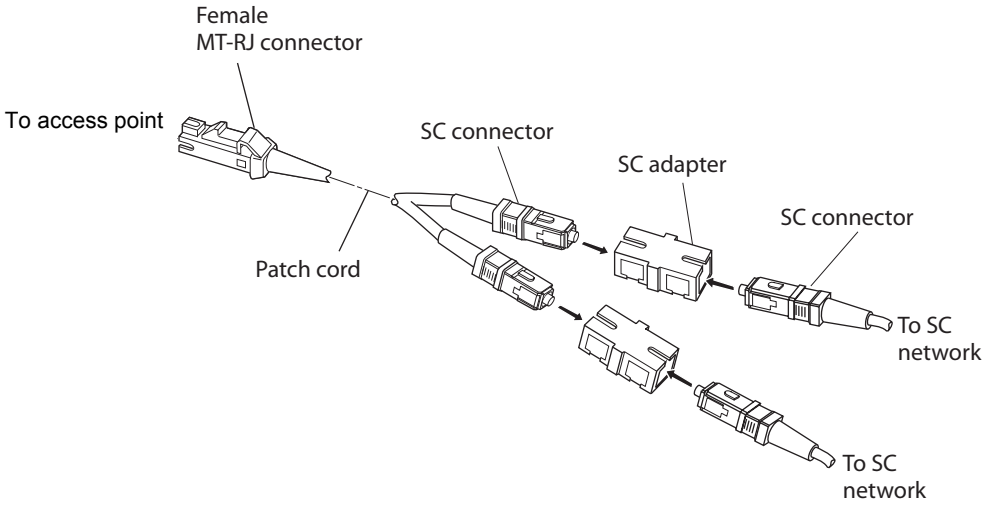
To connect to an SC network

1. Remove any cable protectors attached to the patch cord and adapter.

2. Connect the access point to your network as shown in the next two illustrations.



Note
The patch cord shown above must connect to the access point with a female MT-RJ connector. For details, see "Using and Purchasing the Required Patch Cord and Adapter" on page 55.



Note
The patch cord shown above must connect to the access point with a female MT-RJ connector. For details, see "Using and Purchasing the Required Patch Cord and Adapter" on page 55.

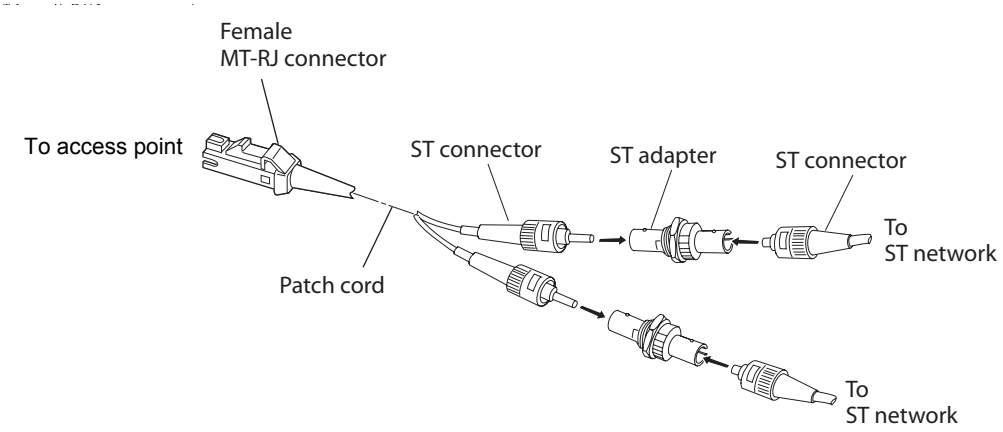
Connecting to an ST Network

To connect to an ST network, you need:

- ❒ a patch cord with a female MT-RJ connector to insert into the access point's male MT-RJ fiber optic port, and an ST connector to insert into the ST adapter.
- ❒ an adapter for connecting the patch cord to the ST network.

To connect to an ST network

1. Remove any cable protectors attached to the patch cord and adapter.
2. Connect the access point to your network as shown in the next illustration.



Note
The patch cord shown above must connect to the access point with a female MT-RJ connector. For details, see "Using and Purchasing the Required Patch Cord and Adapter" on page 55.

Connecting Power Over Ethernet

The AT-WA7500 is powered by power over Ethernet. The AT-WA7501 can be powered by AC power or by power over Ethernet or both. For all access points, you need a power bridge. For a list of the power bridges that Allied Telesyn sells, contact your local Allied Telesyn representative.

This illustration shows how you connect the AT-WA7500 to a power bridge with a typical Ethernet cable to run power over Ethernet.

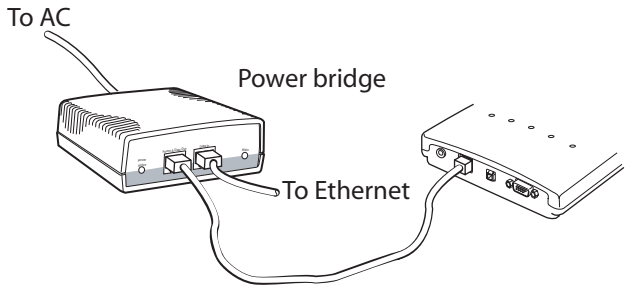


Figure 19. Power Over Ethernet

To connect power over Ethernet

1. Install the power bridges. For help, see the documentation that shipped with the power bridge.

2. Use an Ethernet cable to connect the power bridge to the Ethernet port of the access point.

External Antenna Placement Guidelines

Antennas and their placement play a vital role when installing a wireless network. Every wireless network environment presents its own unique obstacles. Therefore, the exact range that you will achieve with each access point is difficult to determine. Allied Telesyn recommends that you allow an Allied Telesyn-certified RF specialist to perform a site survey before you install a wireless network. For more information, contact your local Allied Telesyn representative.

Radio signals may reflect off some obstacles and be absorbed by others. For example, two radios may achieve up to 305 m (1,000 ft) of range if positioned outdoors within line of sight, with no obstacles between them. However, the same two radios may only achieve 152 m (500 ft) of range when the RF signal has to travel through items such as cubicles. If the signal must penetrate office walls, the signal range may decrease to 91 m (300 ft).

Using the proper antennas for your environment and placing them in the proper areas can help improve range. For information about antenna options, contact your local Allied Telesyn representative. Here are some general guidelines for positioning antennas:

- Place the antenna as high as possible. In an office environment, try to place it above cubicle walls.
- Keep the line-of-sight between the antennas and wireless end devices clear of metal surfaces (like beams or girders) and large quantities of paper products.
- Do not place a sheet of metal (such as a filing cabinet) between two antennas.

These next sections provide detailed information about antenna placement for those access points that can have more than one antenna.

Connecting Antennas to the Radios

All radios have two ports. The radio in slot 2 uses ports 3 and 4, and the radio in slot 2 uses ports 1 and 2. If you have only one radio in the access point, it is in slot 1.

Positioning Antennas for 802.11g, 802.11b, and 802.11a Radios

For the 802.11g and 802.11b radios, the primary port is a transmit/receive port and the secondary port is a receive-only port. The primary port is the right connector (2 or 4) and the secondary port is the left connector (1 or 3). If you only attach one antenna to the 802.11g or 802.11b radio, you must attach it to the primary port.

For the 802.11a radio, both ports are automatically transmit/receive ports, You can attach antennas to both ports and it will automatically use antenna diversity or you can attach one antenna to either port.

Allied Telesyn recommends that you use two antennas for each radio to achieve optimal performance (antenna diversity) of the radios.

Positioning Antennas for Dual Radio Access Points

In addition to the earlier antenna guidelines, if you have a dual radio access point, you need to also follow these recommendations:

- Cable the antennas at least 3.05 m (10 ft) from the access point.
- If the access point has two of the same type of radio, position the antennas for one of the radios at least 3.05 m (10 ft) from the antennas for the other radio.
- If the access point has two radios that are in the same frequency range, position the antennas for one of the radios at least 3.05 m (10 ft) from the antennas for the other radio.

Positioning Antennas for Antenna Diversity

Antenna diversity lets you attach two antennas to one radio to increase the odds of receiving a better signal on either of the antennas. In addition to the earlier antenna guidelines, if you are connecting two antennas to a radio, you need to also follow these recommendation:

Table 12. Recommended Antenna Separation for Antenna Diversity

Location	Recommended Antenna Separation *
Highly reflective warehouse environment	0.33 m (13 in) or 0.64 m (25 in)
Moderately reflective warehouse environment	0.64 m (25 in), 1.22 m (4 ft), or 1.83 m (6 ft)
Open/Office environment	1.22 m (4 ft) to 3.05 m (10 ft)

* The recommendations in this table apply to omni antennas; if you are using directional antennas, increase the recommended separation between the antennas.

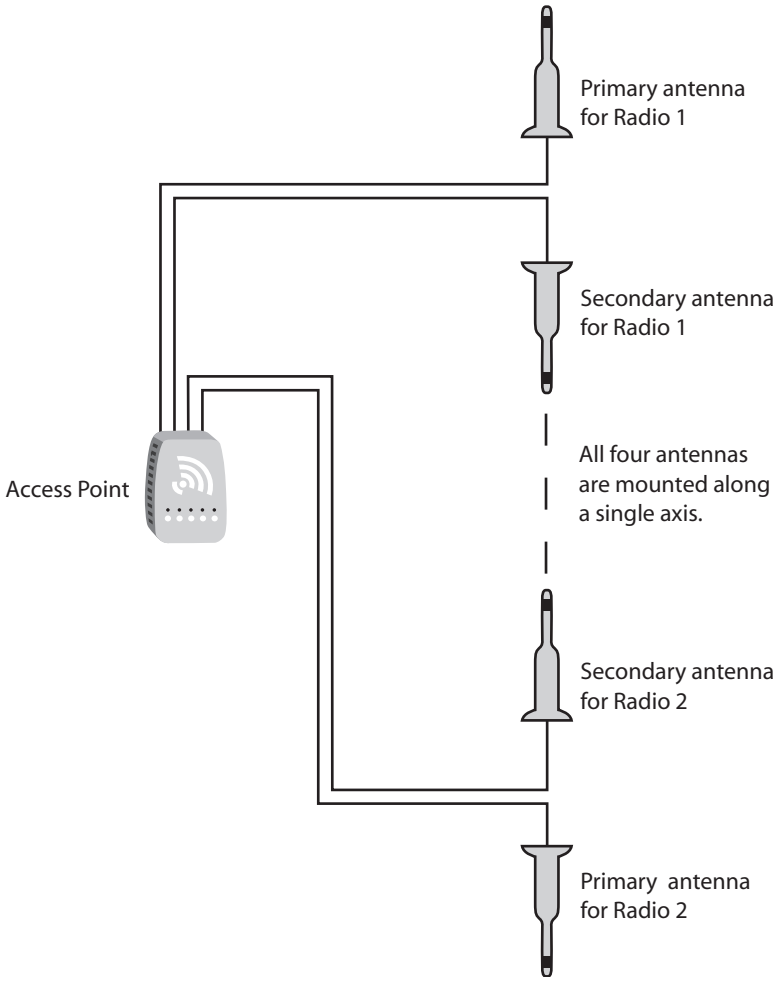
If you are using antenna diversity, where you place each antenna is critical because each antenna has a particular function. Antennas placed too close together may cause interference with each other. Antennas placed too far apart may not be able to establish two-way communications with other radios. Note these important points:

- Position omni antennas for the 802.11b radio at least 0.61 m (2 ft) apart.
- Position directional antennas so they point in the same direction.
- Position the antennas so that both antennas are within range of the radios they need to communicate with.
- Do not position the two antennas around a corner or so that a wall is between them.

- ❒ Follow the recommended antenna separation precisely when using the closest distances. Movement of as little as 3.05 cm (1.2 in) may strongly affect performance. You should choose the greatest distance possible within the constraints of your environment.

Stacked Antenna Positioning for Dual Radio Access Points

As an alternative to the physical separation of omni antennas, you can mount them along a single axis to minimize the antenna-to-antenna coupling.



Note that antenna diversity works differently for 802.11g, 802.11b, and 802.11a radios.

About Antenna Diversity for 802.11g Radios

The 802.11g radios support antenna diversity, but it is not automatically enabled. You must manually enable this feature using the Access Point Configuration menu. From the main menu, click 802.11g Radio > Advanced Configuration. The Antenna Control field, let you choose Diversity.

When antenna diversity is enabled, both ports can receive, but only the primary port transmits. To achieve optimum placement for the two antennas, you must place the transmit/receive antenna so that it is within range of all the radios that the receive-only antenna can hear.

About Antenna Diversity for 802.11b Radios

The 802.11b radios support antenna diversity and it is automatically enabled when you have two antennas connected to one radio. When you are using antenna diversity, both ports can receive, but only the primary port transmits. To achieve optimum placement for the two antennas, you must place the transmit/receive antenna so that it is within range of all the radios that the receive-only antenna can hear.

About Antenna Diversity for 802.11a Radios

The 802.11a radios support antenna diversity and it is automatically enabled. When you have two antennas connected to this radio, both ports can transmit and receive. You can use this feature to provide redundant coverage of the same area covered by the primary antenna or you can use it to provide coverage of a separate area. If you are using directional antennas, you can point them toward different areas or you can place the second antenna on the other side of the wall.

Chapter 3

Configuring the Ethernet Network

This chapter explains how to configure the AT-WA7500 and AT-WA7501 access points so that they communicate with your Ethernet network. This chapter explains:

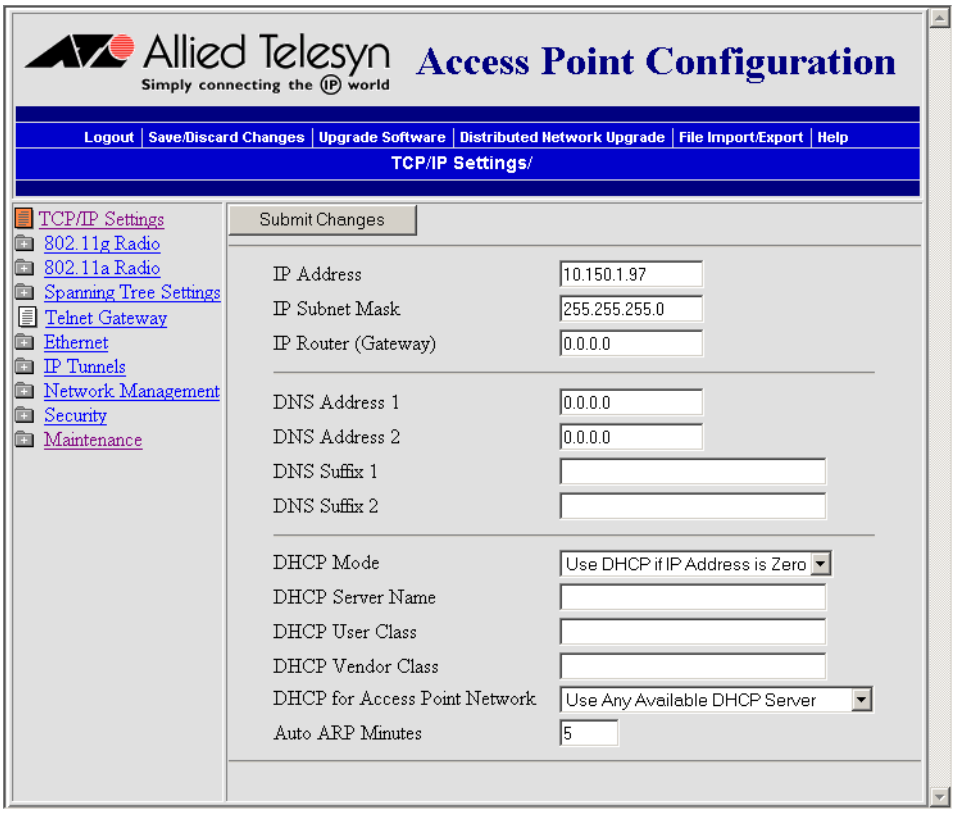
Configuring the TCP/IP Settings

If you are using a DHCP server to automatically assign an IP address to the access point, go to "Configuring the Access Point as a DHCP Client" on page 67. If you are not using a DHCP server, you need to manually assign some TCP/IP parameters.

Note
You should have already configured an IP address for the access point. For help, see "Configuring the Access Point (Setting the IP Address)" on page 38.

To configure the TCP/IP settings

1. From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears.



2. Configure the TCP/IP settings. For help, see the next table.
3. If you want to configure the access point as a DHCP server, see "Configuring the Access Point as a DHCP Server" on page 70.

4. If you want to configure the access point as a NAT server, see “About Network Address Translation (NAT)” on page 75.

5. If you want to configure the access point to send ARP requests, see “Configuring the Access Point to Send ARP Requests” on page 76.

6. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

Table 13. TCP/IP Settings Descriptions

Parameter	Explanation
IP Address	Enter the IP address of the access point. The IP address has the form x.x.x.x, where x is a number from 0 to 255.
IP Subnet Mask	Enter the subnet mask that matches the other devices in your network. The subnet mask has the form x.x.x.x, where x is a number from 0 to 255. If you use DHCP to obtain an IP address for this access point, the subnet mask that is obtained from DHCP will supersede this one.
IP Router (Gateway)	Enter the IP address of the router that will forward frames if the access point will communicate with devices on another subnet. The IP address has the form x.x.x.x, where x is a number from 0 to 255.
DNS Address 1	Enter the IP address of a domain name server that the access point uses to resolve DNS names. If this access point is a DHCP server, this DNS address will be distributed to DHCP clients. You can enter up to two DNS addresses to be delivered to DHCP clients.
DNS Address 2	Enter the IP address of a domain name server that the access point uses to resolve DNS names if the DNS server at DNS Address 1 is not responding. If this access point is a DHCP server, this DNS address will be distributed to DHCP clients.

Table 13. TCP/IP Settings Descriptions (Continued)

Parameter	Explanation
DNS Suffix 1	Enter a domain name suffix that will be appended to DNS names that cannot be resolved. If the access point is a DHCP server, this is the only DNS suffix that is delivered to DHCP clients. For example, enter a suffix of UVW.COM. When you try to resolve ABC, the DNS will look for ABC.UVW.COM.
DNS Suffix 2	Enter a domain name suffix that will be appended to DNS names that cannot be resolved either by themselves or using DNS suffix 1. For example, enter a suffix of XYZ.COM. When you try to resolve ABC, the DNS will first look for ABC.UVW.COM and then it will look for ABC.XYZ.COM.

Configuring the Access Point as a DHCP Client

You can use a DHCP server to automatically assign an IP address and other TCP/IP settings to your access point; that is, the access point can act as a DHCP client.

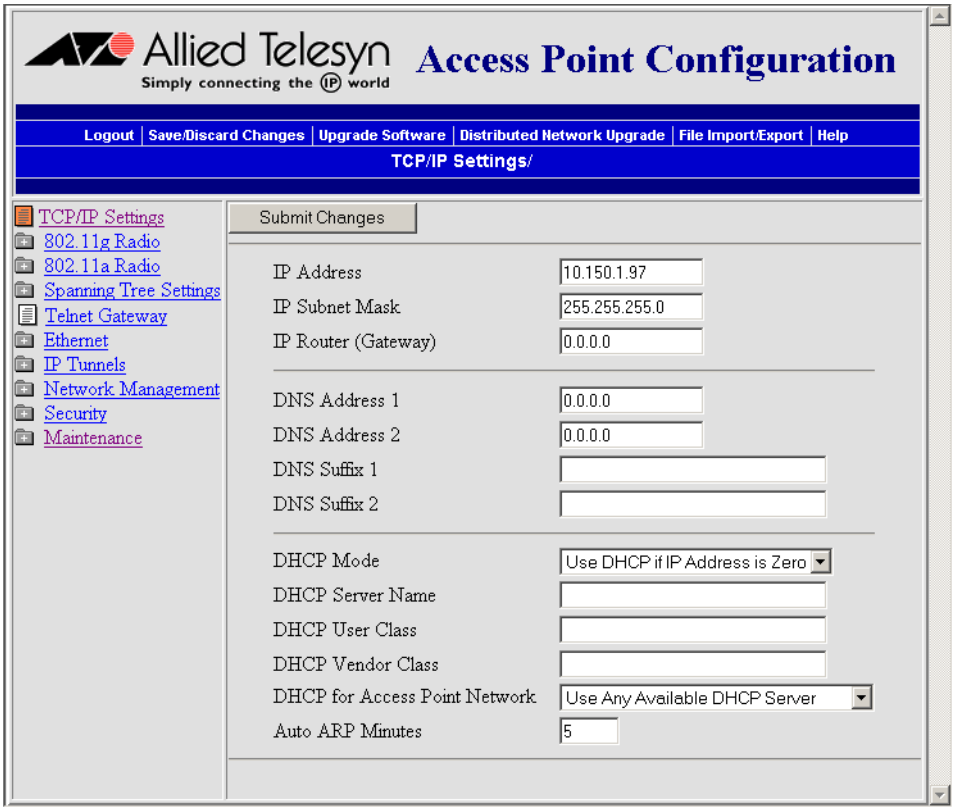
A DHCP client accepts offers from DHCP or BOOTP servers. Preference is given to DHCP servers. If a BOOTP reply is received before a DHCP offer, the access point waits 4 seconds. If a DHCP offer is received within the 4 seconds, the DHCP offer is used and the BOOTP reply is ignored. (BOOTP offers are treated like infinite DHCP leases.)

Note
You cannot configure the access point as both a DHCP server and a DHCP client.

Note
If you are using the embedded authentication server feature, do not configure the access point as a DHCP client.

To configure the access point as a DHCP client

1. From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears.



2. Configure the DHCP parameters to make this access point a DHCP client. For help, see the next table.

Note
If you set DHCP Mode to Disable DHCP and the IP address for this access point is 0.0.0.0, all IP communications are disabled for this access point.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Table 14. DHCP Client Parameter Descriptions

Parameter	Explanation
DHCP Mode	To configure the access point as a DHCP client, you must choose one of these options: Always Use DHCP: The access point uses DHCP after every reboot whether or not an infinite lease was granted in a previous session. If this option is not selected, infinite leases are stored in non-volatile memory and reused after each reboot. (BOOTP is treated like an infinite lease.) Use DHCP if IP Address is Zero: (Default.) The access point uses DHCP only if the IP Address is 0.0.0.0. If you choose this option, make sure that the IP Address is 0.0.0.0.
DHCP Server Name	Leave this field blank if you want the access point to respond to offers from any server. Or enter the name of the DHCP server that this access point accesses for information. This access point will not respond to any other DHCP server.
DHCP User Class	Leave the field blank if you do not want the DHCP client to include a user class identifier in its requests. Or enter the DHCP user class identifier as defined in RFC 3004. When this access point acts as a DHCP client, the string entered in this field is sent in DHCP option 77 in DHCP request messages.
DHCP Vendor Class	Leave the field blank if you do not want the DHCP client to include the vendor class identifier in its requests. Or enter the DHCP vendor class identifier as defined in RFC 2132. When this access point acts as a DHCP client, the string entered in this field is sent in DHCP option 60 in DHCP request messages.

Table 14. DHCP Client Parameter Descriptions (Continued)

Parameter	Explanation
DHCP for Access Point Network	Determines which DHCP servers may be used by access points and wireless devices: **Use Any Available DHCP Server:** Access points and wireless devices may receive DHCP responses and addresses from any available DHCP server. **Only Use Access Point DHCP Server:** Access points and any associated wireless devices may receive DHCP responses and addresses only from an access point DHCP server. Currently, the DHCP server must be located in the root access point. If this option is selected and the root access point does not have a DHCP server enabled, access points and wireless devices will not be able to receive a DHCP address. You can use this option, in combination with a DHCP user class, to segment a network that has an existing DHCP server and an access point DHCP server.

Configuring the Access Point as a DHCP Server

You can configure the access point as a simple DHCP server that provides DHCP server functions for small installations where no other DHCP server is available. The DHCP server will offer IP addresses and other TCP/IP settings to any DHCP client it hears as long as a pool of unallocated IP addresses is available. These clients may include other access points, wireless end devices, wired hosts on the distribution LAN, or wired hosts on secondary LANs.

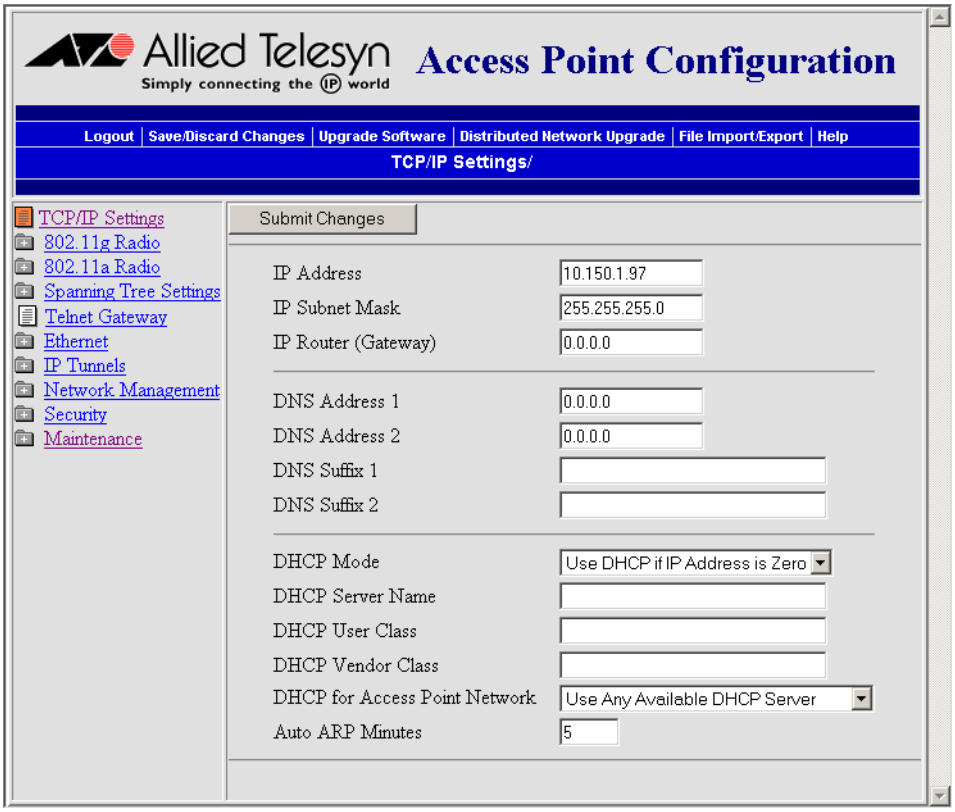
Note
If you configure the access point as a DHCP server, it is not intended to replace a general purpose, configurable DHCP server, and it makes no provisions for synchronizing DHCP policy between itself and other DHCP servers. Customers with complex DHCP policy requirements should use other DHCP server software.

Note
You cannot configure the access point as both a DHCP server and a DHCP client.

To avoid a single point of failure, you can configure more than one access point to be a DHCP server; however, the access points do not share DHCP client databases. You should configure each DHCP server with a different address pool from which to allocate client IP addresses.

To configure the access point as a DHCP server

1. From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears.



2. Verify that the IP Address field, IP Subnet Mask field, and IP Router field are configured. For help, see "Configuring the TCP/IP Settings" on page 65.

3. Configure the DHCP parameters to make this access point a DHCP server. For help, see the next table.

Table 15. DHCP Server Parameter Descriptions

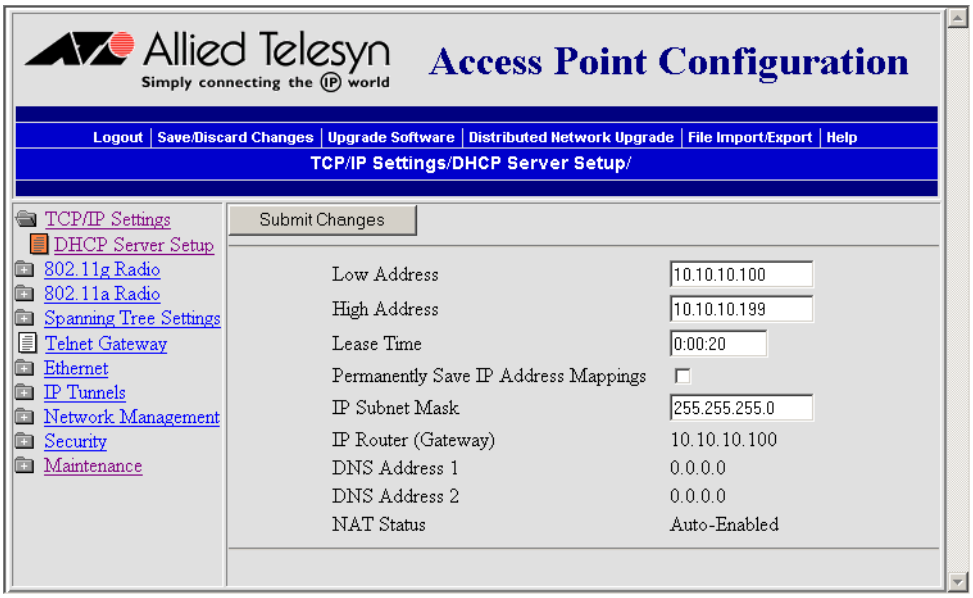
Parameter	Explanation
DHCP Mode	Choose This AP is a DHCP Server. The access point must have a valid IP address and subnet mask.
DHCP Server Name	Enter the name for this access point as a DHCP server.

Table 15. DHCP Server Parameter Descriptions (Continued)

Parameter	Explanation
DHCP User Class	Leave the field blank if you want this access point to respond to requests from any client. Or enter the DHCP user class identifier as defined in RFC 3004. When this access point acts as a DHCP server, the access point offers addresses to client requests only when the client requests contain a matching user class identifier.
DHCP Vendor Class	Leave the field blank if you want this access point to respond to requests from any client. Or enter the DHCP vendor class identifier as defined in RFC 2132. When this access point acts as a DHCP server, the access point offers addresses to client requests only when the client requests contains a matching vendor class identifier.
DHCP for Access Point Network	Determines which DHCP servers may be used by access points and wireless devices: Use Any Available DHCP Server: Access points and wireless devices may receive DHCP responses and addresses from any available DHCP server. Only Use Access Point DHCP Server: Access points and any associated wireless devices may receive DHCP responses and addresses only from an access point DHCP server. Currently, the DHCP server must be located in the root access point. If this option is selected and the root access point does not have a DHCP server enabled, access points and wireless devices will not be able to receive a DHCP address. You can use this option, in combination with a DHCP user class, to segment a network that has an existing DHCP server and an access point DHCP server.

4. Click Submit Changes to save your changes. DHCP Server Setup appears in the menu.

5. From the menu, click DHCP Server Setup. The DHCP Server Setup screen appears.



6. Configure the DHCP server. For help, see the next table.

7. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Table 16. DHCP Server Setup Parameter Descriptions

Parameter	Explanation
Low Address	Enter the low IP address in the range of IP addresses available to the DHCP server for distribution to DHCP clients. If these addresses are not on the same subnet as the access point, the access point will perform Network Address Translation (NAT) for the clients to which it grants IP addresses.
High Address	Enter the high IP address in the range of IP addresses available to the DHCP server for distribution to DHCP clients. If these addresses are not on the same subnet as the access point, the access point will perform Network Address Translation (NAT) for the clients to which it grants IP addresses.

Table 16. DHCP Server Setup Parameter Descriptions (Continued)

Parameter	Explanation
Lease Time	Specifies the duration of the leases that are granted by the DHCP server. Enter the lease time in the format days:hours:minutes. If you set the lease time to 0, infinite leases are granted.
Permanently Save IP Address Mappings	If you check this check box, the DHCP server stores permanent mappings of IP addresses to DHCP client identifiers. A DHCP client is guaranteed to receive the same IP address each time it requests an address even if the DHCP server reboots. If you clear this check box, the DHCP server tries to grant clients the same address each time, but that result is not guaranteed.
Display-only parameters	
IP Subnet Mask	Displays the subnet mask entered at the TCP/IP Settings screen.
IP Router (Gateway)	Displays the address of the IP Router.
DNS Address 1	Displays the IP address of the Domain Name Server. This address will be used for name solution and will be distributed to DHCP clients when this access point is a DHCP server.
DNS Address 2	Displays the IP address of the Domain Name Server. This address will be used for name solution and will be distributed to DHCP clients when this access point is a DHCP server.
NAT Status	This informative entry lets you know if DHCP has been properly configured, and if the range of addresses has automatically enabled Network Address Translation (NAT).

Supported DHCP Server Options

When the access point is acting as a DHCP server, it issues IP address leases to configure the IP address, along with the DNS addresses, DNS suffixes, IP subnet mask, and IP router. These parameters will contain the same values as those configured for the access point.

Unsupported DHCP Server Options

When the access point is acting as a DHCP server, it does not support any DHCP options other than those listed. The DHCP server disregards any DHCP options that are not explicitly required by the DHCP specification. The DHCP server ignores all frames with a non-zero giaddr (gateway IP address). The DHCP server only responds to requests from its own subnet.

About Network Address Translation (NAT)

NAT allows IP addresses to be used by more than one end device. The access point can act as a NAT server, which instantaneously rewrites IP addresses and port numbers in IP headers so that frames all appear to be coming from (or going to) the single IP address of the access point instead of the actual source or destination.

When an end device uses the access point as an IP router, the access point replaces the IP header, which includes the device MAC address, IP source address, and TCP/UDP port, with its own. You can configure the DHCP server to indicate that the access point is the IP router when the server allocates an IP address. Special consideration is given to changing the FTP data connection TCP port number, which is in the body of the TCP frame. After the frame source is modified, it is forwarded to the proper subnet.

If the destination subnet is a different subnet from the one the access point is on, the destination MAC address is changed to the IP router that has been configured for the access point. If the destination subnet is the same subnet as the one the access point is on, the access point converts the MAC address to the MAC address that belongs to the destination IP address. This may involve using ARP for MAC address discovery.

When the access point receives a frame with its IP address, it identifies the need for address translation by inspecting the destination port number. If the port number is within the pool reserved for NAT operation, it looks up the original MAC address, IP address, and port number. The frame is then modified and forwarded to the end device.

NAT operation is disabled or enabled automatically depending on the continuous range of addresses you enter into the DHCP server. NAT is disabled if the range of addresses to be given to DHCP clients is on the same subnet as the access point. NAT is enabled if the range of addresses to be given to DHCP clients is not on the same subnet as the access point; thus, you are creating a virtual network and the DHCP server will also perform NAT translation.

When NAT operation is enabled, the access point uses the low address in the range of addresses as its own. The DHCP/NAT clients also use this address as their router IP address. These clients can configure the access point using this internal IP address or the normal external IP address.

To configure the access point as a NAT server

1. From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears.
2. Verify that the IP Address field and IP Subnet Mask field are configured. For help, see “Configuring the TCP/IP Settings” on page 65.
3. In the DHCP Mode field, choose This AP is a DHCP Server.
4. Click Submit Changes to save your changes.
5. Click DHCP Server Setup and enter a range of IP addresses that are not on the same subnet as the access point.
6. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

Configuring the Access Point to Send ARP Requests

ARP requests are multicast frames, which means they are sent to all devices on the Ethernet network. You can configure the access point to periodically send an unsolicited ARP request to the IP router so that all routers can update their routing tables. This ARP request lets a network management program learn about the access point on the network by querying routers. The auto ARP minutes parameter controls the time interval between ARP requests.

If the address of the IP router is 0.0.0.0, then the access point sends an ARP request to its own IP address. Without this option, an access point might not use its IP address for extended periods of time and the IP address would expire from the router ARP table. If the IP address expires, the network management program must ping all potential addresses on a subnet to locate active IP addresses or require the user to enter a list. You should not let the IP address for the access point expire.

To set the auto ARP period

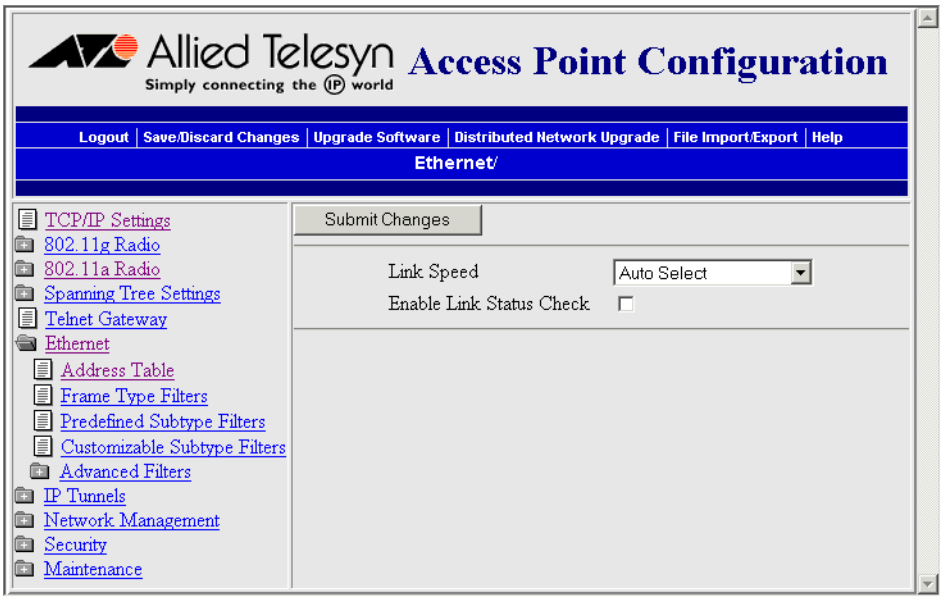
1. From the menu, click TCP/IP Settings. The TCP/IP Settings screen appears.
2. In the Auto ARP Minutes field, enter a time period from 1 to 120 minutes. To disable this parameter, enter 0.
3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

Configuring Other Ethernet or Fiber Optic Settings

Many of the standard Ethernet or fiber optic settings are configured in the TCP/IP Settings screen. For help, see "Configuring the TCP/IP Settings" on page 65. In the Ethernet screen, you can set the port type, set the link speed, and enable or disable the link status check.

To configure the Ethernet or fiber optic settings

1. From the main menu, click Ethernet. The Ethernet screen appears.



2. Configure the parameters. For help, see the next table.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Table 17. Ethernet Parameter Descriptions

Parameter	Explanation
Port Type	Appears only if the access point has a fiber optic port. This field specifies the port that the access point uses to communicate with the Ethernet network: 10/100 Mb Twisted-Pair: The access point communicates with the Ethernet network through the Ethernet port. 100 Mb Fiber Optic: The access point communicates with the Ethernet network through the fiber optic port.
Link Speed	If Port Type is 100 Mb Fiber Optic, this field is automatically set to 100 Mbps Fiber Optic (full duplex). Choose the speed and duplex mode you want this port to use to communicate with the Ethernet. If you want the access point to auto-negotiate this field, choose Auto Select. Auto Select should work for most networks.
Enable Link Status Check	Check this check box if you want the access point to periodically check its Ethernet connection. If it loses the connection, this access point can no longer be the root access point and any end devices that are connected to this access point (whether or not it is the root) will roam to a different access point. The access point will attempt to reconnect to the spanning tree through one of its radio ports. Clear this check box if this access point must be the root access point or if it is used as a WAP.

Configuring the Ethernet Address Table

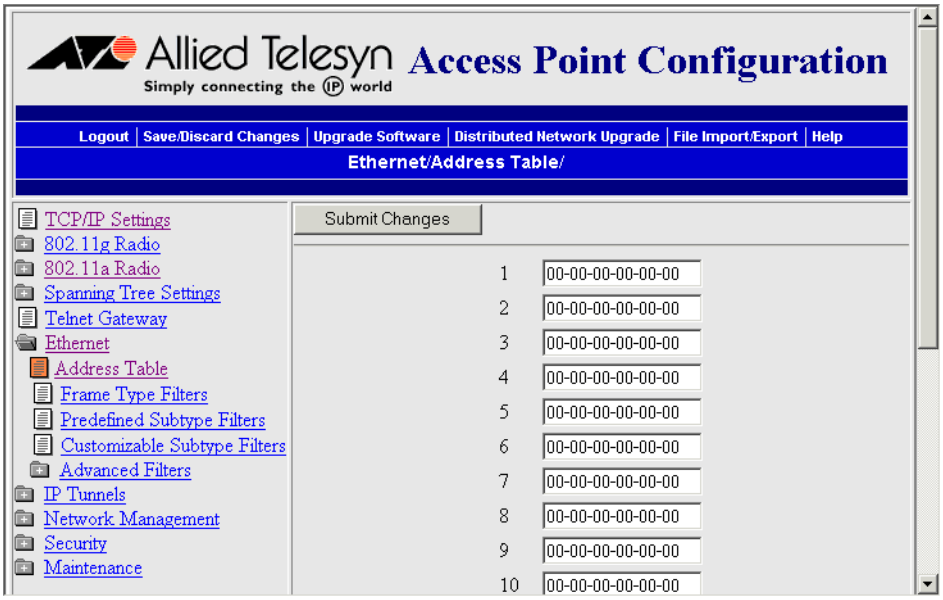
If you have a secondary LAN, you should configure the Ethernet address table in the designated bridge or WAP on the secondary LAN. This table contains all the MAC addresses on the secondary LAN that are communicating with the primary LAN. You must enter the MAC addresses of all devices on the secondary LAN that do not always initiate communication.

If you choose not to configure this table, the designated bridge or WAP may need to flood frames to the Ethernet and radio ports to learn the path to the MAC address.

These addresses become permanent entries in the forwarding table of the designated bridge or WAP.

To configure the Ethernet address table

1. From the main menu, click Ethernet > Address Table. The Address Table screen appears.



2. Enter up to 20 MAC addresses. MAC addresses consist of six hex pairs that are separated by spaces, colons, or hyphens.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Configuring Ethernet Filters

You can set both Ethernet and IP tunnel filters, and you can create protocol filters for both predefined and user-defined protocol types. In addition, you can define arbitrary frame filters based on frame content. Setting Ethernet filters prevents the Ethernet port from sending out unnecessary traffic to the wireless network.

Ethernet frame type filter and predefined subtype filter settings override customizable subtype filter settings. However, Allied Telesyn recommends that when creating customizable subtype filters, you do not duplicate existing frame type or predefined subtype filters or unexpected results may occur.

For more examples of using Ethernet filters and for help configuring IP filters, see “Configuring IP Tunnel Filters” on page 150.

Using Ethernet Frame Type Filters

You can define filters for common networking protocols such as IP, Novell IPX, and 802.2 LLC. You can also set filters that will pass only those Ethernet frame types found on your network.

You can set the default action for general and specific frame types. For example, you cannot pass the DIX-Other EtherTypes frame parameter and then use the subtype menus to pass only those specific DIX types that are used in your radio network.

You can also set the scope for general and specific frame types. For example, for DIX-IP-TCP ports, you cannot pass all frame types. Then, all IP frames with the TCP type will be dropped even if specific TCP parts are set to pass in the subtype menus.

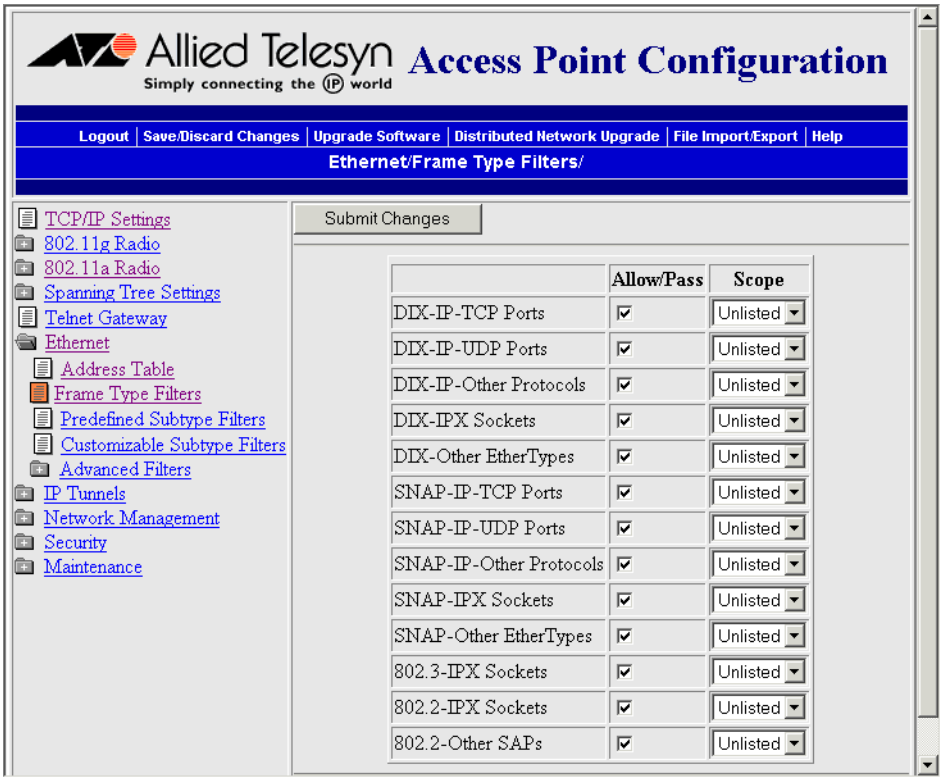
Here is the action and scope you can set for each parameter:

Allow/Pass: Check or clear this check box. Check the check box to pass all frames of that type. Clear the check box to drop all frames of that type.

Scope: Set scope to Unlisted or All. If you select All, then all frames of that type are unconditionally passed or dropped, depending on the action you specified. If you select Unlisted, then frames are passed or dropped only if the frame type is not listed in the predefined or customizable tables.

To set frame type filters

1. From the main menu, click Ethernet > Frame Type Filters. The Frame Type Filters screen appears.



2. For each frame type field, check or clear the Allow/Pass check box to configure if the frame types are allowed to pass or are dropped. If you check the check box, the frame type is allowed to pass. For help, see the next table.

3. For each frame type field, set the Scope field to Unlisted or All. For help, see the next table.

4. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

5. If you set the Scope field to Unlisted for any of the frame types, you must also configure predefined subtype filters or customizable subtype filters. For help, see the next section, “Using Predefined Subtype Filters” on page 83 or “Customizing Subtype Filters” on page 83.

Table 18. Frame Type Filter Descriptions

Frame Type	Explanation
DIX IP TCP Ports DIX IP UDP Ports SNAP IP TCP Ports SNAP IP UDP Ports	Primary Internet Protocol Suite (IP) transport protocols.
DIX IP Other Protocols SNAP IP Other Protocols	IP protocols other than TCP or User Datagram Protocol (UDP).
DIX IPX Sockets	Novell NetWare protocol over Ethernet II frames.
SNAP IPX Sockets	Novell NetWare protocol over 802.2 SNAP frames.
802.3 IPX Sockets	Novell NetWare protocol over 802.3 RAW frames.
DIX Other Ethernet Types SNAP Other Ethernet Types	DIX or SNAP registered protocols other than IP or IPX.
802.2 IPX Sockets	Novell running over 802.2 Logical Link Control (LLC).
802.2 Other SAPs	802.2 SAPs other than IPX or SNAP.

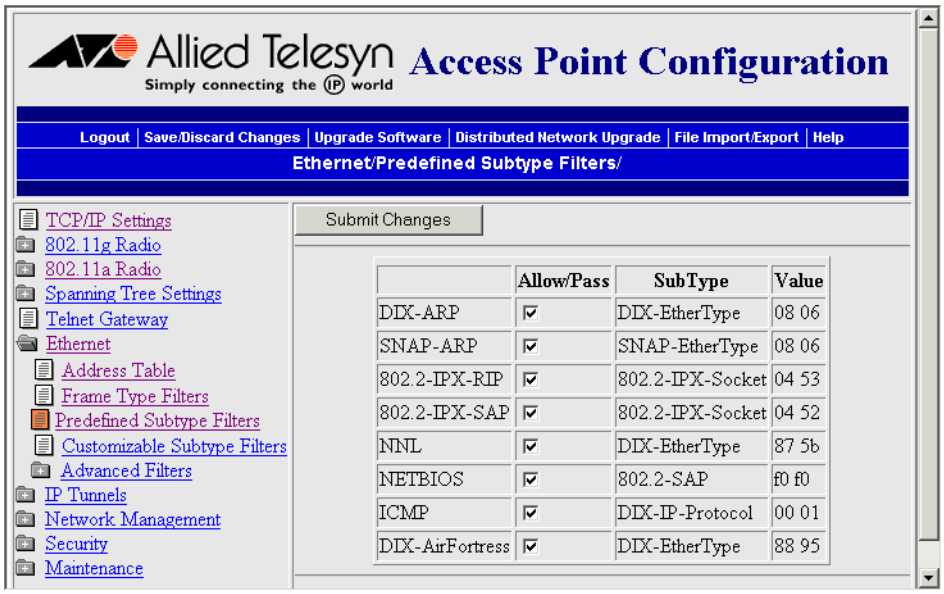
Note
You should not filter HTTP, Telnet, SNMP, and ICMP frames if you are using WAPs because these frame types are used for configuring, troubleshooting, and upgrading WAPs.

Using Predefined Subtype Filters

You can configure the access point to pass or drop certain predefined frame subtypes.

To configure predefined subtype filters

1. From the main menu, click Ethernet > Predefined Subtype Filters. The Predefined Subtype Filters screen appears.



2. For each frame subtype field, check or clear the Allow/Pass check box to configure if the frame subtypes are allowed to pass or are dropped. If you check the check box, the frame subtype is allowed to pass.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Customizing Subtype Filters

You can configure the access point to pass or drop certain customized frame subtypes. You define the action, subtype, and value parameters:

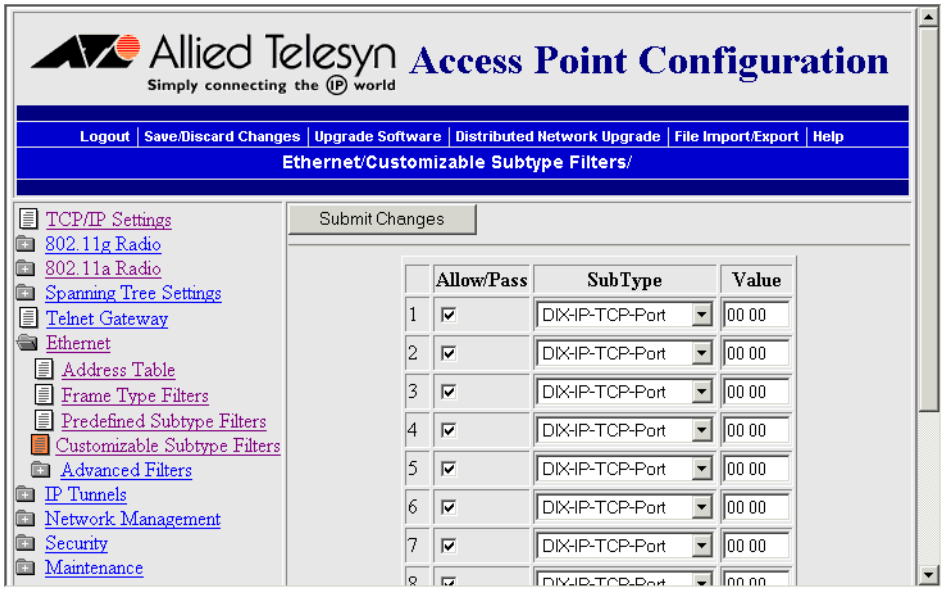
Allow/Pass: Check or clear this check box. Check this check box to pass all frames of the subtype and value. Clear this check box to drop all frames of the subtype and value.

SubType: Selects the frame subtype you wish to configure. For help setting the subtype and value, see the Table 19, "Subtype Filter Descriptions" on page 84.

Value: The value must be two hex pairs. When a match is found between frame subtype and value, the specified action is taken.

To customize subtype filters

1. From the main menu, click Ethernet > Customizable Subtype Filters. The Customizable Subtype Filters screen appears.



2. For each subtype field, check or clear the Allow/Pass check box to configure if the subtypes are allowed to pass or are dropped. If you check the check box, the subtype is allowed to pass.

3. In the SubType field, choose the customizable frame subtype. For help, see the next table.

4. In the Value field, enter the two hex pairs. For help, see the next table.

5. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

Table 19. Subtype Filter Descriptions

SubType	Value
DIX-IP-TCP-Port	Port value in hexadecimal.
DIX-IP-UDP-Port	Port value in hexadecimal.
DIX-IP-Protocol	Protocol number in hexadecimal.
DIX-IPX-Socket	Socket value in hexadecimal.
DIX-EtherType	Specify the registered DIX type in hexadecimal.
SNAP-IP-TCP-Port	Port value in hexadecimal.

Table 19. Subtype Filter Descriptions (Continued)

SubType	Value
SNAP-IP-UDP-Port	Port value in hexadecimal.
SNAP-IP-Protocol	Port value in hexadecimal.
SNAP-IPX-Socket	Socket value in hexadecimal.
SNAP-EtherType	SNAP type in hexadecimal. To filter on both SNAP type and OUI, use advanced filters.
802.3-IPX-Socket	Socket value in hexadecimal.
802.2-IPX-Socket	Socket value in hexadecimal.
802.2-SAP	802.2 SAP in hexadecimal.

Example

This example shows you how to use customizable filters to allow only the wireless end devices (DHCP clients) communicating with the access point (DHCP server) to receive TCP/IP settings. This example prevents the wireless end devices from receiving TCP/IP settings from another DHCP server on the Ethernet network. It also prevents the access point from providing TCP/IP settings to DHCP clients on the wired network.

For this example, set these customizable subtype filters.

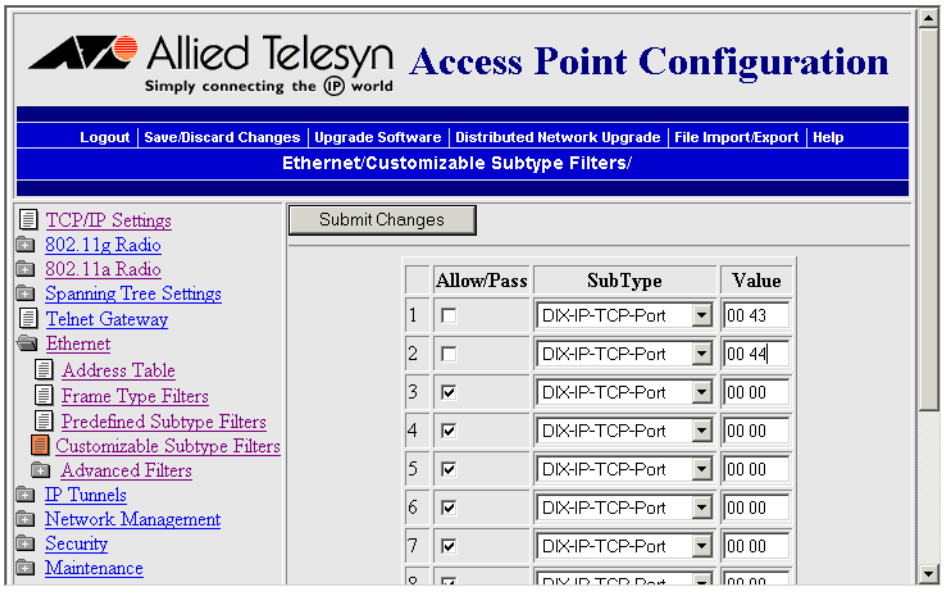


Table 20. Example – Customizable Subtype Filter

Filter	Parameter	Value	Explanation
1	Allow/Pass	Clear (drop)	This filter drops DHCP responses to wireless end devices communicating with this access point.
	Subtype	DIX-IP-UDP-Port	
	Value	00 43	
2	Allow/Pass	Clear (drop)	This filter drops DHCP requests from DHCP clients on the Ethernet network.
	Subtype	DIX-IP-UDP-Port	
	Value	00 44	

Configuring Advanced Filters

You can configure advanced filters if you need more flexibility in your filtering. Settings for advanced filters execute after those for other filters; that is, advanced filters are only applied if the frame has passed the other filters.

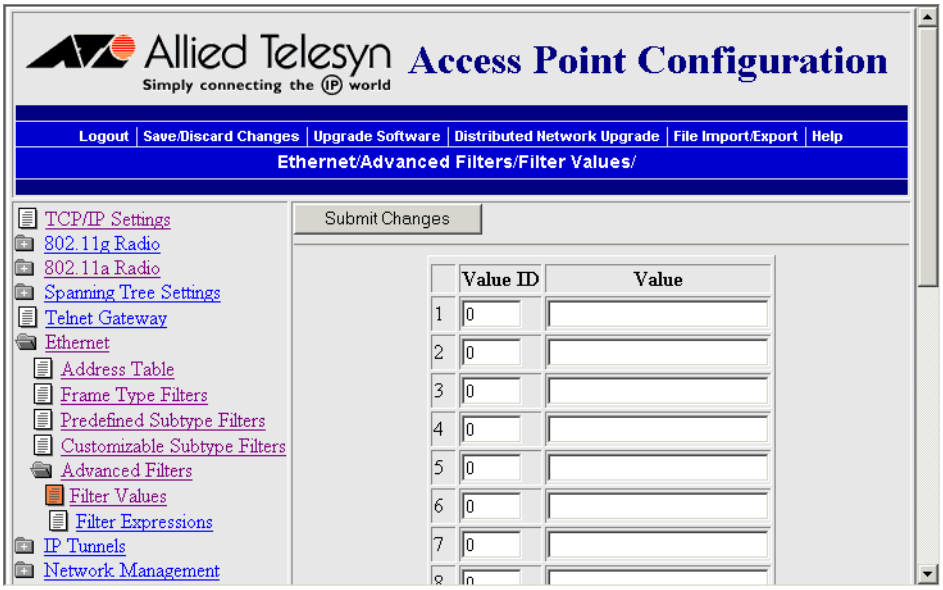
You can use filter values and filter expressions to minimize network traffic over the wireless links; however, Allied Telesyn recommends that you use advanced Ethernet filters only if you have an extensive understanding of network frames and their contents. Use other existing filters whenever possible.

Setting Filter Values

You can associate an ID with a pattern value by selecting a filter and then entering an ID and a value. All values with the same value ID belong to the same list.

To set the value ID and value

1. From the main menu, click Ethernet > Advanced Filters. The Filter Values screen appears.



2. Enter up to 22 value IDs and values.

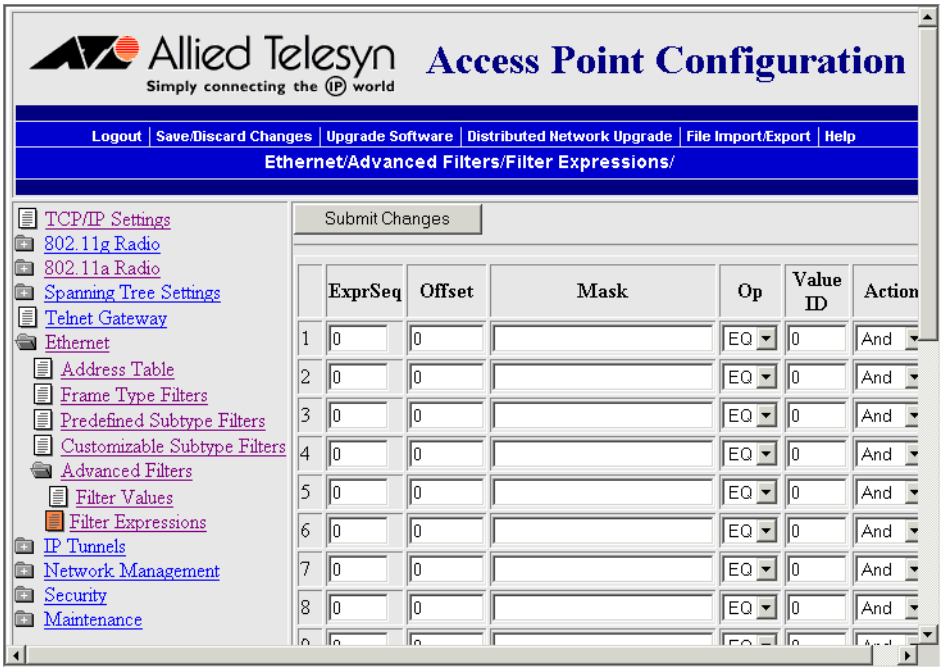
3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Setting Filter Expressions

You can set filter expressions by specifying parameters for frame filters. You can also create a filter expression, which is executed in ascending order based on the ExprSeq values until the access point determines whether to pass or drop the frame.

To set filter expressions

1. From the main menu, click Ethernet > Advanced Filters > Filter Expressions. The Filter Expressions screen appears.



2. Configure the filter expressions parameters. For help, see the next table.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

Table 21. Filter Expressions Parameter Descriptions

Parameter	Explanation
ExprSeq (Expression Sequence)	Indicates the order in which the filters will be executed. When you change the parameter, the statements are reordered and renumbered so the Expression Sequence order is maintained. The range is from 0 to 255. This parameter works with the Action parameter; for example, if the action is set to And, then the next sequence in another expression is processed.
Offset	Identifies a point inside the frame where testing for the expression is to start. The range is from 0 to 65535.

Table 21. Filter Expressions Parameter Descriptions (Continued)

Parameter	Explanation
Mask	Applies a data pattern to the frame. If the data pattern in the mask matches the frame, then the specific action is performed. The mask indicates the bits that are significant at the specified offset. A bit is significant if a bit in the mask is set to one. If this field is empty, the length of the field is determined by the longest value in the Filter Values menu for the specified value ID. The mask values are entered in 0 to 8 hexadecimal pairs.
Op (Operation)	Performs a logical operation when a data pattern matches a value in the Filter Values menu to determine if the specified action should be taken. Valid operations include: EQ (equal), NE (not equal), GT (greater than), LT (less than or equal)
Value ID	Represents a value in the Filter Values menu. The bytes after the frame offset are compared to the data pattern indicated by the value. Value ID can be from 0 to 255 and must match one or more value IDs in the Filter Values menu.
Action	Sets the action to Pass, Drop, or And. If you set the action to And, the filter expression with the next highest sequence is applied.

Example 1

This example shows you how to use Ethernet filters to filter all traffic that passes through the access point to the wireless network except for traffic for specified MAC addresses. These filters do not prevent wireless traffic from reaching the Ethernet network. For this example, set these filter values.

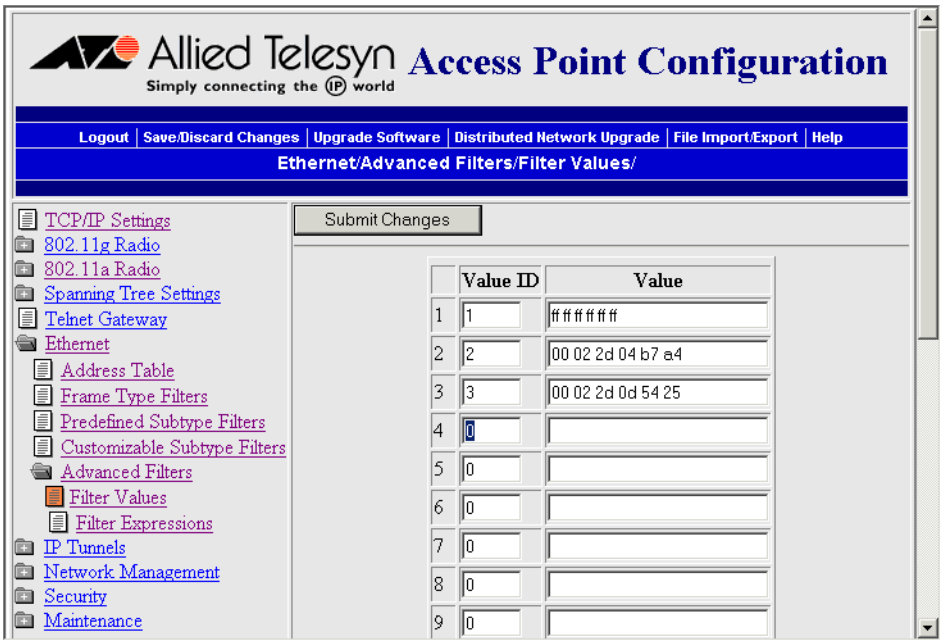


Table 22. Example 1 - Filter Values

Value ID	Value	Description
1	ff ff ff ff ff ff	Allows multicast traffic to enter the wireless network, which is necessary for IP end devices to communicate
2	00 02 2d 04 b7 a4	The MAC address of an end device you want to be able to communicate.
3	00 02 2d 0d 54 25	The MAC address of an end device you want to be able to communicate.

For this example, set these filter expressions.

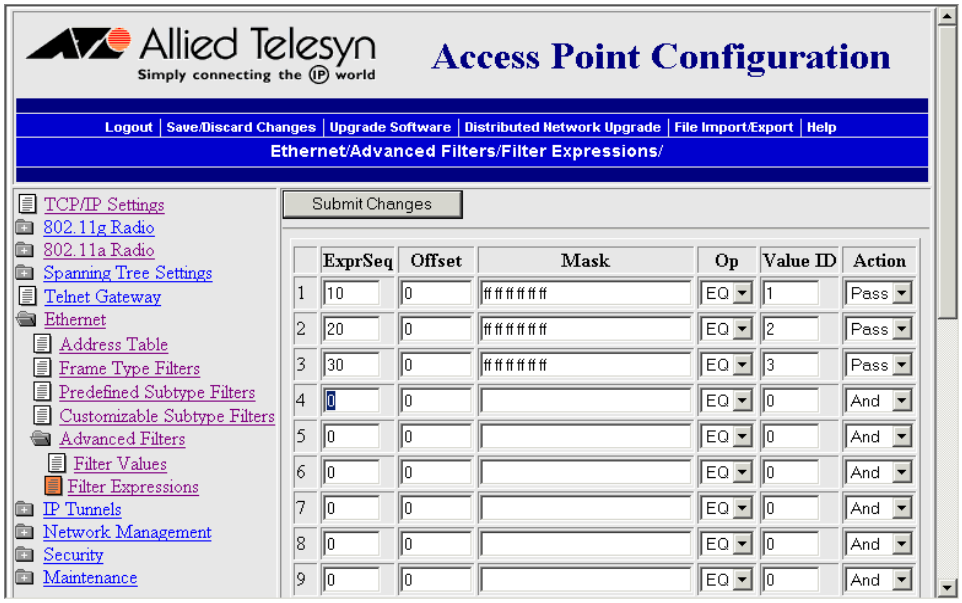


Table 23. Example 1 – Filter Expressions

Parameter	Value	Explanation
ExprSeq	10	The order that you want the expressions executed. You must have an expression for each Value ID that is listed in the Filter Values menu.
Offset	0	Since the filter is applied to the destination address, which is the first value in the frame, the offset is 0.
Mask	ff ff ff ff ff ff	Compares the entire 6-byte destination address for an exact match.
Op	EQ	Compares the value after the offset and mask are applied to the value of the Value ID from the Filter Values menu to see if they are equal. (If the value at the offset equals the specified value on the Filter Values menu, the frame is multicast.)
Value ID	1	This filter expression applies to value ID 1 from the Filter Values menu.
Action	Pass	If this filter expression is true, continue to the next expression.

You must enter a filter expression for each Value ID in the Filter Values menu. In this example, only the ExprSeq and the Value ID values change.

Example 2

This example shows how to use Ethernet filters to discard all DIX IP multicast frames except those from selected devices. Three entries have a value ID of 3 to demonstrate how to enter a list. All entries with the same value ID belong to the same list. For this example, set these filter values.

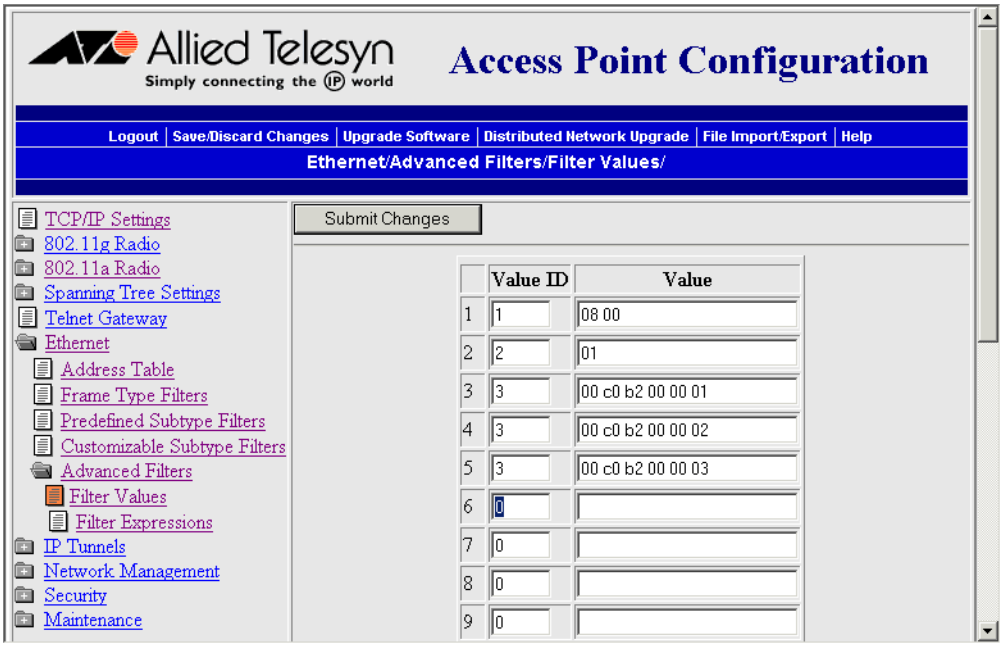


Table 24. Example 2 - Filter Values

Value ID	Value	Description
1	08 00	Check for a DIX IP frame.
2	01	Check for a multicast frame.
3	00 c0 b2 00 00 01 00 c0 b2 00 00 02 00 c0 b2 00 00 03	Check for these specific MAC device addresses.

You must enter a filter expression for each Value ID in the Filter Values menu. In this example, three expressions combine to form a single compound expression. The compound expression forms an advanced filter that drops all DIX IP multicast frames except those from the three Ethernet stations whose addresses are listed on the Filter Values menu.

The default action is the opposite of the action specified in the last expression. In this example, the action of the last expression is drop; therefore, the default action is pass. Any frame that meets the conditions specified in the advanced filter is passed.

Set the first filter expression as shown below.

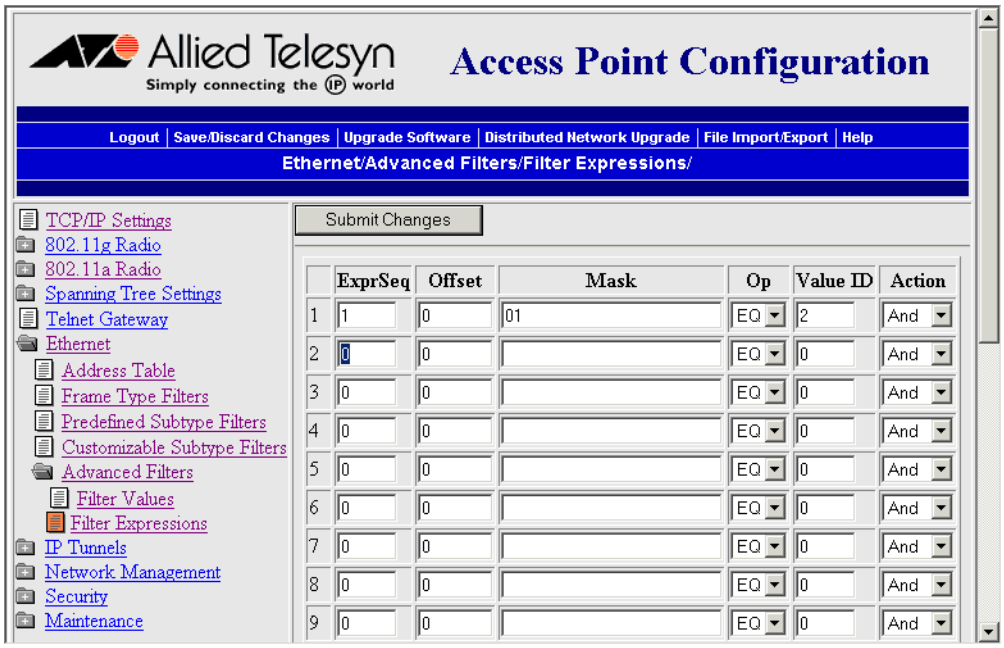


Table 25. Example 2 – First Filter Expression

Parameter	Value	Explanation
ExprSeq	1	The first expression that is executed. You must have an expression for each Value ID that is listed in the Filter Values menu.
Offset	0	Since the filter is applied to the destination address, which is the first value in the frame, the offset is 0.
Mask	01	Checks only the Ethernet multicast bit.
Op	EQ	Compares the value after the offset and mask are applied to the value of the Value ID from the Filter Values menu to see if they are equal. (If the value at the offset equals the specified value on the Filter Values menu, the frame is multicast.)
Value ID	2	This filter expression applies to value ID 2 from the Filter Values menu.
Action	And	If this filter expression is true, continue to the next expression.

Set the second filter expression as shown below.

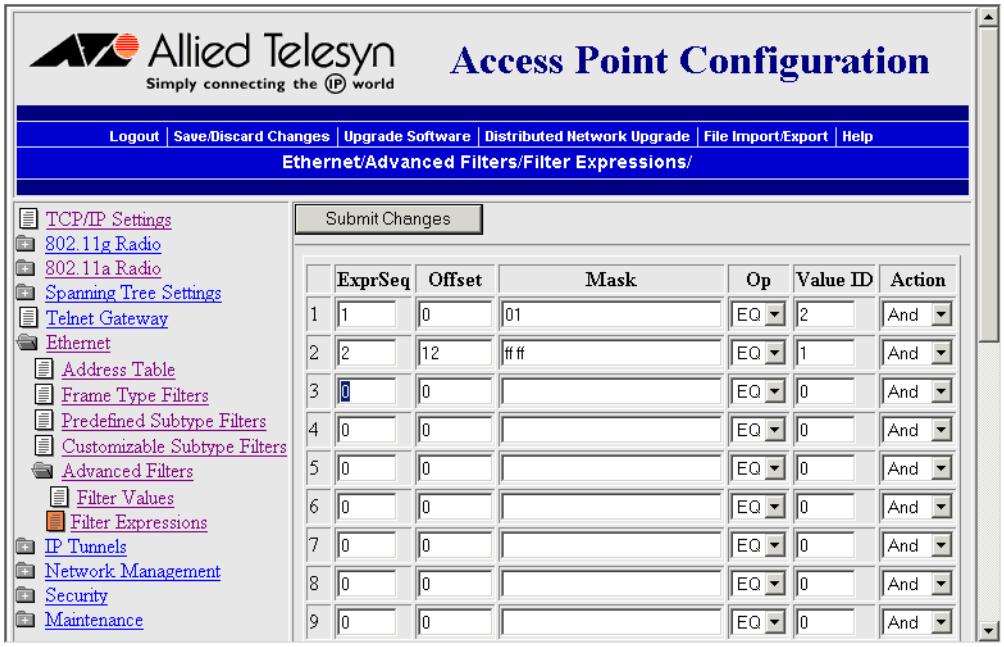


Table 26. Example 2 – Second Filter Expression

Parameter	Value	Explanation
ExprSeq	2	The second expression that is executed.
Offset	12	Checks for the DIX IP frame type, which starts 12 bytes from the destination address.
Mask	ff ff	Checks the 2-byte DIX IP frame type for an exact match.
Op	EQ	Compares the value after the offset and mask are applied to the value of the Value ID from the Filter Values menu to see if they are equal. (If the value at the offset equals the specified value on the Filter Values menu, the frame is DIX IP.)
Value ID	1	This filter expression applies to value ID 1 from the Filter Values menu.
Action	And	If this filter expression is true, continue to the next expression.

Set the third filter expression as shown below.

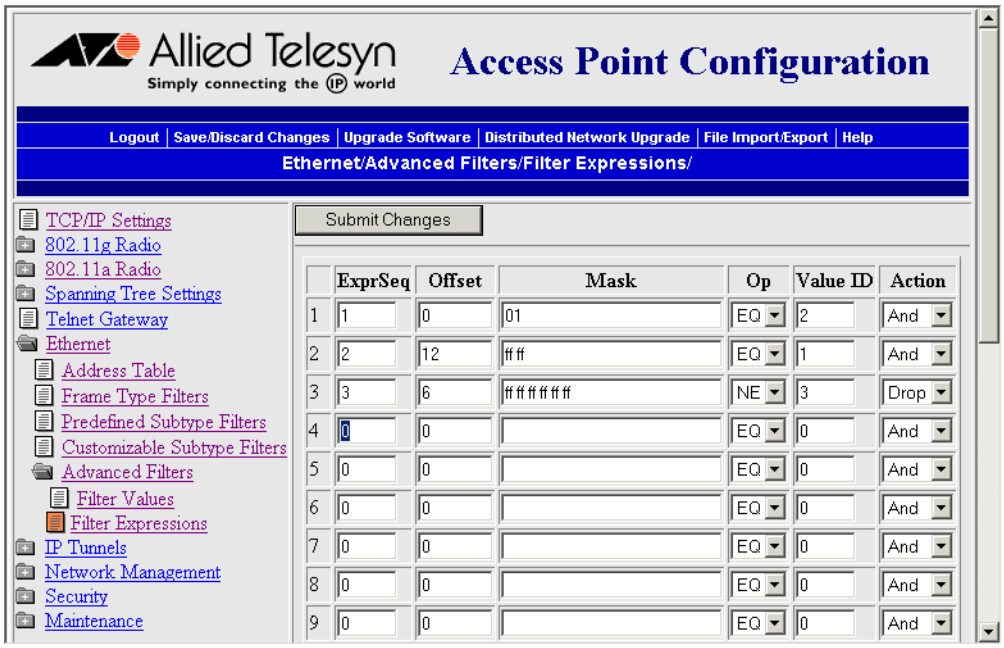


Table 27. Example 2 – Third Filter Expression

Parameter	Value	Explanation
ExprSeq	3	The third expression that is executed.
Offset	6	Checks the source Ethernet address, which starts 6 bytes from the destination address.
Mask	ff ff ff ff ff ff	Checks the 6-byte source Ethernet address for an exact match.
OP	NE	Compares the value after the offset and mask are applied to the value of the Value ID from the Filter Values menu to see if they are not equal. (Compare the source Ethernet address with the list of MAC addresses from the Filter Values menu.)
Value ID	3	This filter expression applies to value ID 3 from the Filter Values menu.
Action	Drop	If the source Ethernet address does not match any address in the list on the Filter Values menu, then drop the frame.

Chapter 4

Configuring the Radios

This chapter explains how to configure the radios in the AT-WA7500 and AT-WA7501 access points so that they communicate with your wireless end devices. This chapter covers these topics:

About the Radios

The AT-WA7500 and AT-WA7501 access products may contain one or two radios. You can use access points that contain two different types of radios to support two different types of wireless networks, such as legacy networks. You can use access points with two of the same type of radios as WAPs, as point-to-multipoint bridges, to increase throughput in a busy network, or to provide redundancy.

Table 28. Access Point Radios Supported and Features

Access Point	Radio Supported			Dual Radio Support	Radio Independent
	802.11g*	802.11b	802.11a		
WA7500	Yes	Yes	Yes	Yes	Yes
WA7501	Yes	Yes	Yes	Yes	Yes

* The 802.11g radio is sometimes referred to as the 802.11b/g because it can be configured to communicate with any 802.11b and 802.11g radios that have the same SSID and security settings.

The next sections explain how to configure the radios that are in your access point. Only the radios actually installed in your access point appear in the configuration menus.

Configuring the 802.11g Radio

You can configure the 802.11g radio to communicate with other 802.11g and 802.11b radios that have the same:

- SSID (Network Name)
- Security

For each radio, you can assign up to four service sets, creating one primary service set and up to three secondary service sets. Each service set shares the same Advanced Configuration and Inbound Filters settings, but you can customize the security settings. However, most clients do not support a mixed security environment using multiple service sets:

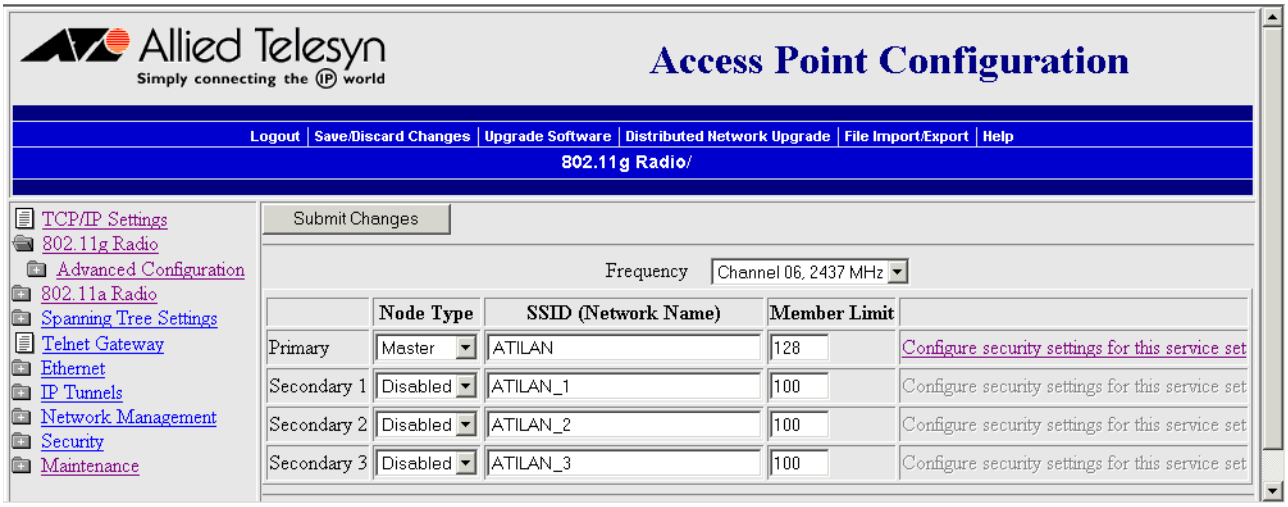
- If you configure security on the primary service set, then you should also configure security on the secondary service sets.
- If you do not configure security on the primary service set, then you cannot configure security on the secondary service sets.

For details, see “When You Configure Different SSIDs with Different Security Settings” on page 172.

Multiple service sets are used primarily to allow one physical radio to support multiple virtual LANs (VLANs). For details about VLANs, see “Configuring VLANs” on page 187.

To configure the 802.11g radio

1. From the main menu, click 802.11g Radio. The 802.11g Radio screen appears.



2. Configure the parameters for the radio. For help, see the next table.

3. Configure the advanced parameters for the radio. For help, see "Configuring 802.11g Radio Advanced Parameters" on page 102.

4. (Master only) Configure inbound filters. For help, see "Configuring 802.11g Radio Inbound Filters" on page 107.

5. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

6. (Optional) Configure security by clicking Configure security settings for this service set. For help, see Chapter 6, "Configuring Security" on page 169.

Table 29. 802.11g Radio Parameter Descriptions

Parameter	Explanation
Frequency (Master radio only)	Choose the frequency that this access point uses to transmit and receive frames. The available frequencies depend on the country and the radio option configured on the access point. See the Table 30, "Worldwide Frequencies for 802.11g and 802.11b Radios" on page 101. You may want to use a single frequency to isolate the installation to part of the band; for example, use a single frequency if other wireless networks or microwave ovens are in the area. For optimal performance of master radios in access points that are in range of each other, configure the frequencies to be at least five channels apart. For example, configure the frequency to use channels 1, 6, and 11.

Table 29. 802.11g Radio Parameter Descriptions (Continued)

Parameter	Explanation
Node Type	Configure the 802.11g radio to master, station, or disabled: Master: The radio always operates in Master mode. The radio becomes active to accept connections for wireless devices when the access point joins the spanning tree. All service sets to be configured for a VLAN must be set to Master. Station: The radio always operates in Station mode. The radio searches for an access point with an active Master mode radio to connect to. If a connection is established, this link becomes a possible connection to the root. Disabled: The radio is disabled. You can create up to four service sets for this radio by setting the Node Type as follows: ❒ If the primary service set is Master, up to three secondary SSIDs may be set to Master. ❒ If the primary SSID is Station, all secondary service sets are disabled and do not appear on screen. ❒ If the primary service set is Disabled, all secondary service sets (and the physical radio) are disabled.
SSID (Network Name)	Enter a unique SSID for each enabled service set. You can configure up to four service sets for this radio. The SSID is case sensitive and cannot be more than 32 alphanumeric characters. 802.11g radios can be configured to communicate with other 802.11g and/or 802.11b radios with the same SSIDs. You need to assign the same SSID to the wireless end devices that will connect to the radio.
Member Limit	Controls the maximum number of devices that can be associated with this enabled service set.

Table 30. Worldwide Frequencies for 802.11g and 802.11b Radios

Channel	FCC	ETSI	France	Japan	Israel
1	2412	2412		2412	
2	2417	2417		2417	
3	2422 (default)	2422 (default)		2422 (default)	2422 (default)
4	2427	2427		2427	
5	2432	2432		2432	
6	2437	2437		2437	
7	2442	2442		2442	
8	2447	2447		2447	
9	2452	2452		2452	
10	2457	2457	2457	2457	
11	2462	2462	2462 (default)	2462	
12		2467	2467	2467	
13		2472	2472	2472	
14				2484	

The 802.11g and 802.11b channels that are allowed in a given country may change without notice. Be sure you use only those frequencies that are permissible in the given country. Note the following:

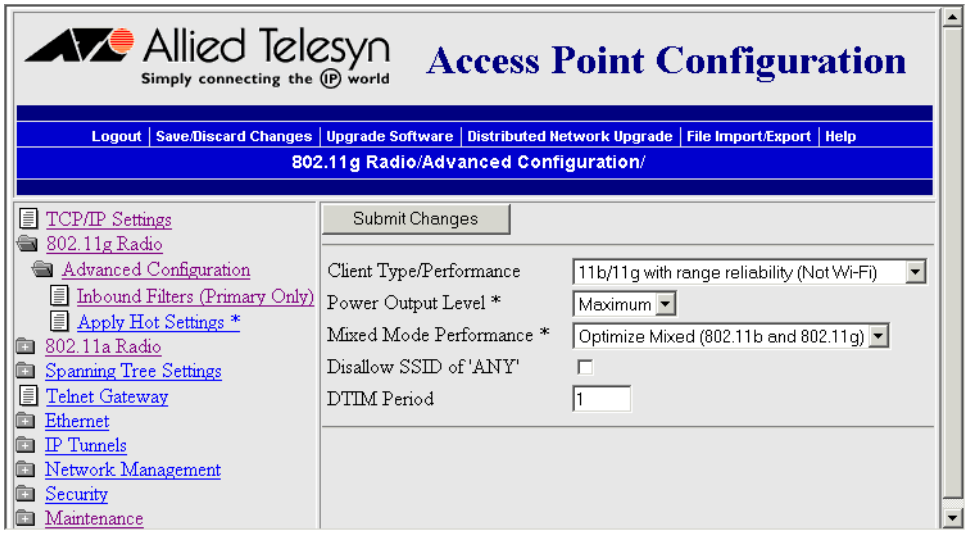
- FCC countries include the United States, Canada, China, Taiwan, India, Thailand, Indonesia, Malaysia, Hong Kong, and most South American countries.
- ETSI countries include all European Union countries except France. It also includes Switzerland, Iceland, Norway, Czech Republic, Slovenia, Slovakia, Turkey, Russia, and the United Arab Emirates.
- France, Mexico, and Singapore use the same channels.

Configuring 802.11g Radio Advanced Parameters

You can configure advanced parameters for the 802.11g radio primary service set. These settings are shared by any secondary service sets defined for the radio.

To configure advanced parameters

1. From the main menu, click 802.11g Radio > Advanced Configuration. The Advanced Configuration screen appears.



2. Configure the advanced parameters. For help, see the next table.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

> **Note**
> If the field name is marked with an asterisk (*), you can immediately activate the changes without rebooting. For help, see “Applying Hot Settings” on page 108.

Table 31. 802.11g Radio Advanced Parameter Descriptions

Parameter	Description
Client Type/Performance	Specifies if this radio will communicate with 802.11b and/or 802.11g radios: 11b/11g with range reliability (Not Wi-Fi): Allows clients with 802.11b or 802.11g radios. Parameters are adjusted for longer range. Basic rates are 1 or 2 Mbps. Extended rates are 6, 12, or 24 Mbps. Data rates are 1, 2, 5.5, or 11 Mbps and extended data rates are 6, 9, 12, 18, 24, 36, 48, or 54 Mbps. 11b/11g with Wi-Fi compatible rates: Allows clients with 802.11b or 802.11g radios. Basic rates are 1, 2, 5.5, or 11 Mbps. Data rates are 1, 2, 5.5, or 11 Mbps. Extended data rates are 6, 9, 12, 18, 24, 36, 48, or 54 Mbps. 11g only for better throughput (Wi-Fi): Only allows clients with 802.11g radios only. Clients without extended rates capabilities are rejected. Basic rates are 1, 2, 5.5, 11, 6, 12, or 24 Mbps. Data rates are 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, or 54 Mbps. 11b/11g using 11b supported rates (Wi-Fi): Allows clients with 802.11b or 802.11g radios. Clients that have mandatory extended data rate requirements will not associate. Basic rates are 1 or 2 Mbps. Data rates are 1, 2, 5, 5, or 11 Mbps.

Table 31. 802.11g Radio Advanced Parameter Descriptions (Continued)

Parameter	Description
Power Output Level*	Set the transmitted power level: Maximum (63 mW): Sets the output power to the highest level supported by the radio. Medium (32 mW): Sets the output power to 3 dB lower than the highest level supported by the radio. Low (16 mW): Sets the output power to a level higher than the minimum level supported by the radio. Minimum (2 mW): Sets the output power to the lowest level supported by the radio. Lowering the power output level reduces the radio coverage for this area and reduces the range for this radio.
Enable Medium Reservation	Determines if you want to set a reservation threshold. Check this check box to set a threshold value. Click Submit Changes, and the Reservation Threshold parameter appears. If you clear this check box, you may improve network response time in installations that usually send very small frames or that have no hidden stations.
Reservation Threshold	Appears only if the Enable Medium Reservation parameter is checked. If you enable medium reservation, you need to set a threshold value, which is the largest data frame that can be transmitted without reserving air time. Air time is normally reserved to help prevent collisions with other transmitters.

Table 31. 802.11g Radio Advanced Parameter Descriptions (Continued)

Parameter	Description
Fragmentation Threshold	Specifies the largest data frame that can be transmitted without fragmentation. Range is 256 to 1600. On certain radios, the fragmentation does not occur unless the radio detects interference. Larger frame sizes can improve throughput on a reliable connection. Smaller frame sizes can improve throughput on a poor connection.
Antenna control*	Specifies whether the radio uses two antennas or one antenna: Two Antennas: The radio selects the antenna for transmission and reception based on best reception. One Antenna: The radio uses only one antenna for transmission and reception.
Mixed Mode Performance*	Optimizes the frame burst window length to optimize performance for specific clients. Gives more time to higher rate frames to maximize throughput in the presence of low rate clients. Range is 0 to 2000. Optimized for 802.11g clients: 802.11g transmissions are maximized. Optimized for 802.11b clients: 802.11b transmissions are maximized. Optimize Mixed (802.11g and 802.11b): Allows an optimal mix of 802.11g and 802.11b transmissions.
Enable Data Rate Fallback	Determines if you want the radio to drop to a slower data rate when it has trouble communicating with another radio.

Table 31. 802.11g Radio Advanced Parameter Descriptions (Continued)

Parameter	Description
Disallow SSID (Network Name) of ‘ANY (Master radio only)	Determines if end devices that have their SSID set to ANY or are left blank (empty) can associate with this radio. Clear this check box to allow these end devices to associate with this radio. Although this setting is 802.11 compliant, it is not very secure. Check this check box to prevent end devices with an SSID of ANY or are left blank from associating with this radio.
DTIM Period (Master radio only)	Specifies the number of beacon periods to skip before including a DTIM (delivery traffic indication message) in a beacon frame. Range is 1 to 65535. Setting a higher DTIM period may conserve battery life in an end device, but it may increase response time.

Configuring 802.11g Radio Inbound Filters

You can configure inbound filters for the 802.11g radio primary service set. These settings are shared by any secondary service sets defined for the radio. You can filter different types of wireless traffic that it may receive. You may want to use this feature by itself or with an access control list (ACL) to help secure your network. If you clear all the check boxes, the radio cannot communicate with any other radios.

You need to check the Allow IAPP check box if you want the access point to be able to communicate with other access points and participate in the spanning tree.

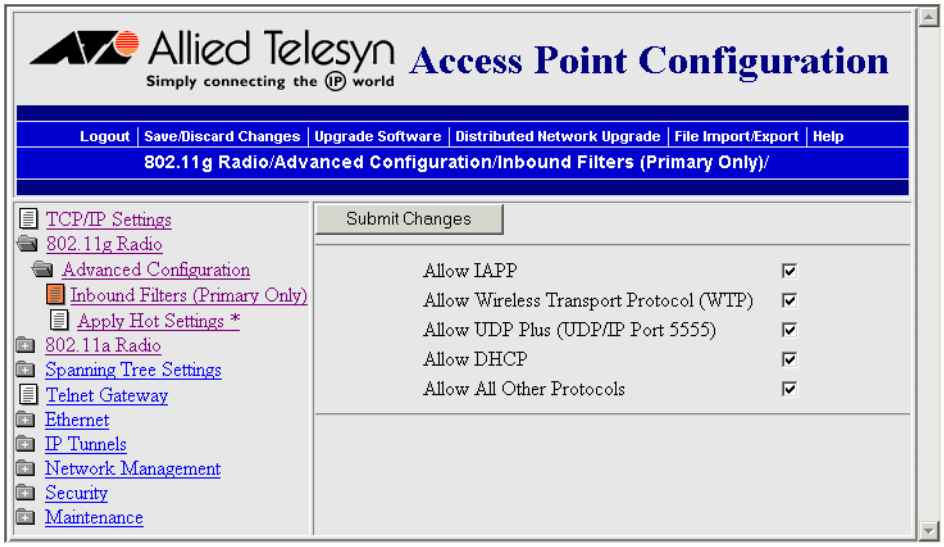
You can use this feature to form a secure wireless hop. Clear all check boxes, except for the Allow IAPP check box.

Or you may want to use this feature in a terminal emulation environment when you know the end devices are sending only UDP Plus or Wireless Transport Protocol (WTP) frames. Check the Allow UDP Plus check box or the Allow Wireless Transport Protocol check box and clear all other check boxes (except the Allow IAPP check box). The access point master radio will only accept the UDP Plus or WTP frames and discard all other frames, which can make a more secure network.

Note
If any of the devices are also DHCP clients, you need to check the Allow DHCP check box.

To configure 802.11g radio inbound filters

1. From the main menu, click 802.11g Radio > Advanced Configuration > Inbound Filters (Primary Only). The Inbound Filters screen appears.



2. For each frame type, check or clear each check box. For help, see the next table.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

Table 32. 802.11g Radio Inbound Filter Descriptions

Parameter	Description
Allow IAPP	Determines if this radio accepts IAPP (Inter Access Point Protocol) frames from other access point station radios. The IAPP frames must match Ethernet protocol 875c.
Allow Wireless Transport Protocol (WTP)	Determines if this radio accepts WTP frames from end devices. The WTP frames must match Ethernet protocol 875b.
Allow UDP Plus (UDP/IP Port 5555)	Determines if this radio accepts UDP Plus frames from end devices. The UDP Plus frames must match the UDP network port 5555 on the DCS 30X, Allied Telesyn Gateway, or ARP.
Allow DHCP	Determines if this radio accepts DHCP frames. The DHCP frames must match UDP destination port 67 and ARP. Check this check box if the end devices are DHCP clients.
Allow All Other Protocols	Determines if this radio accepts all other protocols that are not filtered by one of the filters in this screen.

Applying Hot Settings

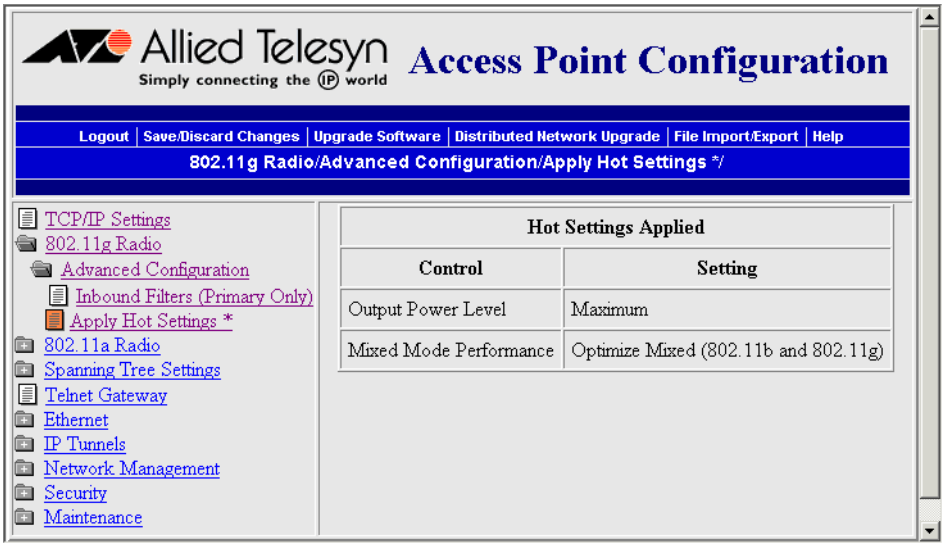
You can “hot set” some advanced parameters (marked with an *), such as Power Output Level, Antenna Control, and Mixed Mode Performance, for the 802.11g radio, which means that the new settings can be immediately activated without rebooting the access point.

To apply hot settings

1. From the main menu, click 802.11g Radio > Advanced Configuration and change the parameters as needed.

2. Click Submit Changes to save your changes to the “current” configuration file (as defined in “Saving Configuration Changes” on page 46).

3. From the main menu, click Apply Hot Settings to save your changes to the "active" configuration file (as defined in "Saving Configuration Changes" on page 46). The Apply Hot Settings screen appears. This screen is read-only.



Configuring the 802.11g Radio to Communicate With a SpectraLink Network

SpectraLink wireless telephone systems simplify network infrastructure and network management by combining voice and data traffic over one wireless network, leveraging 802.11b wireless LAN technology. The 802.11g radio can communicate the SpectraLink network. For more information on the SpectraLink Network, see "Configuring a SpectraLink Network" on page 117.

802.11g radios can support both voice and data communications. You still need to define the normal 802.11g parameters, such as SSID (Network Name) and security.

To configure the 802.11g radio

1. From the main menu, click 802.11g Radio > Advanced Configuration. The Advanced Configuration screen appears.

2. In the Client Type/Performance field, choose 11b/11g with range reliability (Not Wi-Fi).

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

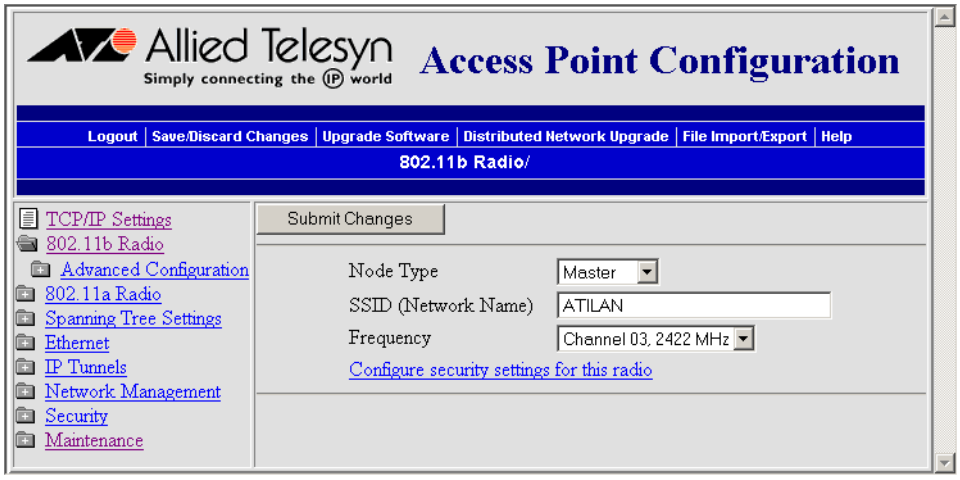
Configuring the 802.11b Radio

The 802.11b radio will communicate with other 802.11b radios that have the same:

- SSID (Network Name)
- Security

To configure the 802.11b radio

1. From the main menu, click 802.11b Radio. The 802.11b Radio screen appears.



2. Configure the parameters for the radio. For help, see the next table.

3. Configure the advanced parameters for the radio. For help, see “Configuring 802.11b Radio Advanced Parameters” on page 112.

4. (Master only) Configure inbound filters. For help, see “Configuring 802.11b Radio Inbound Filters” on page 115.

5. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

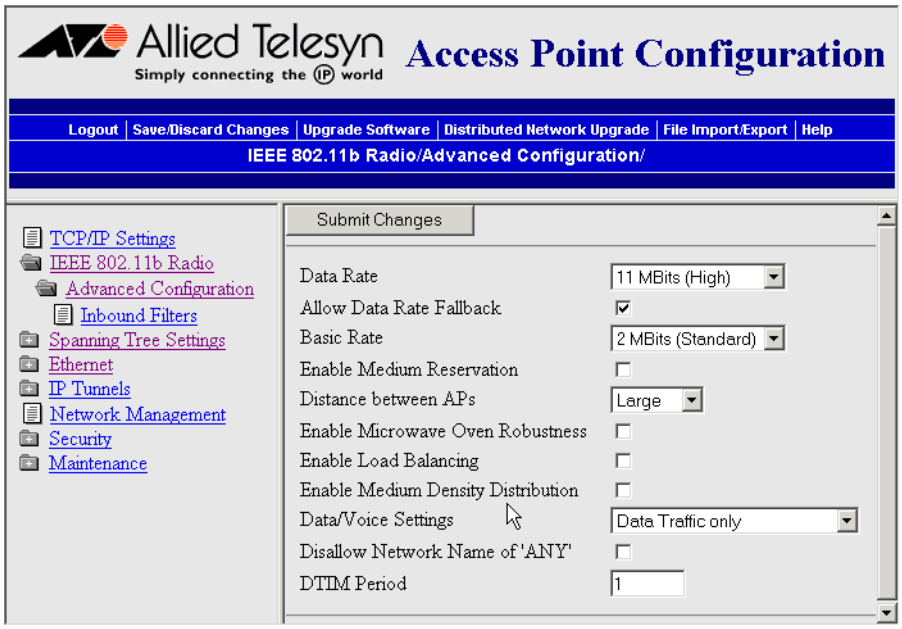
6. (Optional) Configure security by clicking Configure security settings for this radio. For help, see Chapter 6, “Configuring Security” on page 169.

Table 33. 802.11b Radio Parameter Descriptions

Parameter	Description
Node Type	Configure the 802.11b radio as a master or station. You can also disable the radio.
SSID (Network Name)	Enter the SSID (network name) for this radio. The network name is case sensitive and can be no more than 32 alphanumeric characters. 802.11b radios communicate with other 802.11b radios with the same SSID. You need to assign the same SSID to the wireless end devices that will connect to the radio.
Frequency (Master radio only)	Choose the frequency within the 2.4 to 2.5 GHz range that this access point uses to transmit and receive frames. The available frequencies are country-dependent and are determined by the radio. See the Table 30, "Worldwide Frequencies for 802.11g and 802.11b Radios" on page 101. Configure all access points used in Spain, France, or Japan to a common frequency. For all other countries, configure all access points to a common frequency, or select up to three frequencies that are at least three channels (or 25 MHz) apart. For example, you could select 2412 MHz, 2437 MHz, and 2462 MHz. You may want to use a single frequency to isolate the installation to part of the band; for example, use a single frequency if other wireless networks or microwave ovens are in the area. For optimal performance of master radios in access points that are in range of each other, configure the frequencies to be at least five channels apart. For example, configure the frequency to use channels 1, 6, and 11.

Configuring 802.11b Radio Advanced Parameters

1. From the main menu, click 802.11b Radio > Advanced Configuration. The Advanced Configuration screen appears.



2. Configure the advanced parameters. For help, see the next table.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

Table 34. 802.11b Radio Advanced Parameter Descriptions

Parameter	Description
Data Rate	Choose the rate at which the access point transmits data. In general, higher speeds mean shorter range and lower speeds mean longer range. You can set this rate to 11, 5.5, 2, or 1 Mbps.
Allow Data Rate Fallback	Determines if you want the radio to drop to a slower data rate when it has trouble communicating with another radio.

Table 34. 802.11b Radio Advanced Parameter Descriptions (Continued)

Parameter	Description
Basic Rate	Choose the rate at which the access point transmits multicast and beacon frames. In general, higher speeds mean shorter range and lower speeds mean longer range. Do not set this rate higher than the maximum rate at which your end devices can receive multicast frames. You can set this rate to 11, 5.5, 2, or 1 Mbps. This parameter should usually be left at the default 2 Mbps.
Enable Medium Reservation	Determines if you want to specify a reservation threshold. Check this check box to set a threshold value. Click Submit Changes, and the Reservation Threshold parameter appears. If you clear this check box, you may improve network response time in installations that usually send very small frames or that have no hidden stations.
Reservation Threshold	Appears only if the Enable Medium Reservation parameter is checked. If you enable medium reservation, you need to set a threshold value, which is the largest data frame that can be transmitted without reserving airtime. Airtime is normally reserved to help prevent collisions with other transmitters.
Distance Between APs	Controls the roaming sensitivity of your end devices. This setting should match the setting on your end devices. You can use this parameter to virtually reduce the range of your access point. If you choose Small or Medium, you do not reduce the absolute range of your radio, but you modify the collision detection mechanism to allow significant overlap of the wireless cells. Thus, you create a higher performance radio network, but you need more access points to cover an area.
Enable Microwave Oven Robustness	Determines if the access point activates a modified algorithm for automatic rate fallback, which prevents the access point from falling back to 1 Mbps when trying to retransmit radio frames when 2.4 GHz interference is present.

Table 34. 802.11b Radio Advanced Parameter Descriptions (Continued)

Parameter	Description
Enable Load Balancing	Determines if end devices can distribute their connections across multiple access points.
Enable Medium Density Distribution	Determines if these access point parameters—Enable Medium Reservation, Distance Between APs, Enable Microwave Oven Robustness—are distributed to end devices that support this feature.
Data/Voice Settings (Master radio only)	Choose the setting that optimizes the wireless network: Data Traffic Only: The access point transmits only data traffic. Data and SpectraLink Traffic: The access point transmits both data and voice traffic. SpectraLink telephone frames are sent in the high priority queue. Frames in the high priority queue are sent ahead of frames in the normal priority queue. No special filtering. SpectraLink Traffic Only: The access point transmits only voice traffic. SpectraLink telephone frames are sent with a priority setting. All other multicast/broadcast frames are dropped.
Disallow SSID (Network Name) of 'ANY' (Master radio only)	Determines if end devices that have their SSID (Network Name) set to ANY or are left blank can associate with this radio. Clear this check box to allow these end devices to associate with this radio. Although this setting is 802.11 compliant, it is not very secure. Check this check box to prevent end devices with an SSID of ANY or are left blank from associating with this radio.
DTIM Period (Master radio only)	Specifies the number of beacon frames to skip before including a DTIM (delivery traffic indication message) in a beacon frame. Setting a higher DTIM period may conserve battery life in an end device, but it may increase response time.

Configuring 802.11b Radio Inbound Filters

When configuring a master radio, you can filter different types of wireless traffic that it may receive. You may want to use this feature by itself or with an access control list (ACL) to help secure your network. If you clear all the check boxes, the radio cannot communicate with any other radios.

You should check the Allow IAPP check box so the access point can communicate with other access points and participate in the spanning tree.

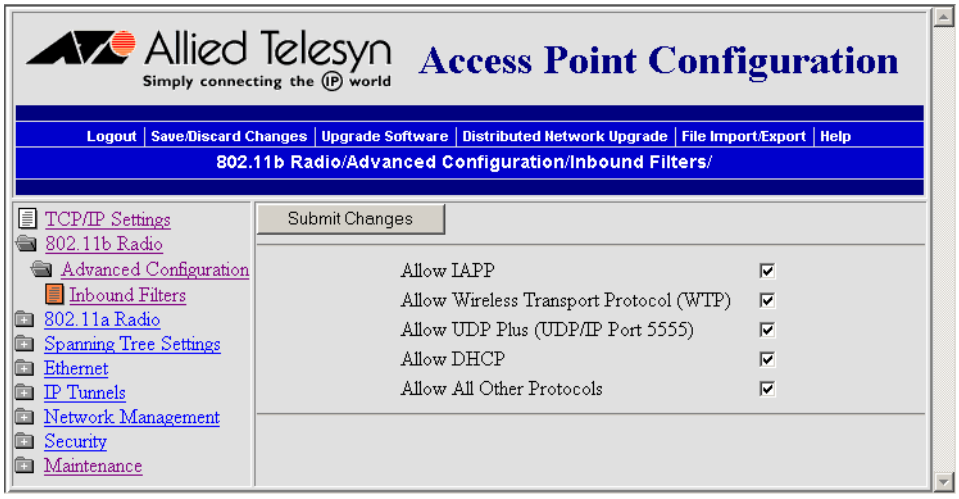
You can use this feature to form a secure wireless hop. Clear all check boxes, except for the Allow IAPP check box.

Or you may want to use this feature in a terminal emulation environment when you know the end devices are sending only UDP Plus or Wireless Transport Protocol (WTP) frames. Check the Allow UDP Plus check box or the Allow Wireless Transport Protocol check box and clear all other check boxes (except the Allow IAPP check box). The access point master radio will only accept the UDP Plus or WTP frames and discard all other frames, which can make a more secure network.

Note
If any of the devices are also DHCP clients, you need to check the Allow DHCP check box.

To configure 802.11b radio inbound filters

1. From the main menu, click 802.11b Radio > Advanced Configuration > Inbound Filters. The Inbound Filters screen appears.



2. For each frame type, check or clear each check box. For help, see the next table.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

Table 35. 802.11b Radio Inbound Filter Descriptions

Parameter	Description
Allow IAPP	Determines if this radio accepts IAPP (Inter Access Point Protocol) frames from other access point station radios. The IAPP frames must match Ethernet protocol 875c.
Allow Wireless Transport Protocol (WTP)	Determines if this radio accepts WTP frames from end devices. The WTP frames must match Ethernet protocol 875b.
Allow SpectraLink Voice Protocol (SVP)	Determines if this radio accepts SVP frames from voice wireless telephones. The SVP frames must match IP 119.
Allow UDP Plus (UDP/IP Port 5555)	Determines if this radio accepts UDP Plus frames from end devices. The UDP Plus frames must match the UDP network port 5555 on the DCS 30X, Allied Telesyn Gateway, or ARP.
Allow DHCP	Determines if this radio accepts DHCP frames. The DHCP frames must match UDP destination port 67 and ARP. Check this check box if the end devices are DHCP clients.
Allow All Other Protocols	Determines if this radio accepts all other protocols that are not filtered by one of the filters in this screen.

Configuring a SpectraLink Network

SpectraLink wireless telephone systems simplify network infrastructure and network management by combining voice and data traffic over one wireless network, leveraging 802.11b wireless LAN technology. You use your SpectraLink telephone to make and receive calls, just like a regular telephone, subject to the restrictions of your PBX.

SpectraLink telephones and gateways operate as adjuncts to existing wireless LANs and PBXs. SpectraLink networks use digital spread spectrum radio technology and integrate with enterprise telephone switching and networking systems. These features provide voice quality throughout the coverage area because there are no clicks, no fading, and no dead spots.

If you are using a SpectraLink network with your ATI access products and wireless data collection network, you need to configure an 802.11b radio port to accept voice traffic. 802.11b radios can support both voice and data communications. You still need to define the normal 802.11b parameters, such as SSID (Network Name) and security.

Table 36. Number of Phones Supported

Number of 802.11b Radios Installed	Number of Phones Supported (Voice Only)	Number of Phones Supported (Voice and Data)
2	14 (7 per radio) Both radios are set to voice traffic only.	7 Set one radio to voice traffic only. Dedicate the other radio to data traffic only or to data and voice traffic.
1	7	7

To configure a SpectraLink network Note

Note
If your access point contains dual radios, use a different SSID (Network Name) for each radio so you can specify which end devices/telephones attach to which radio. You also must enter the Network Name on each telephone.

1. 1 From the main menu, click 802.11b Radio > Advanced Configuration. The Advanced Configuration screen appears.

2. In the Data/Voice Settings field, choose either Data and SpectraLink Traffic or SpectraLink Traffic Only. For help, see “Configuring 802.11b Radio Advanced Parameters” on page 112.

3. Check the Allow Data Rate Fallback check box.

4. In the Basic Rate field:

   - ❒ if you are using a 2 Mbps SpectraLink telephone, set it to 2 Mbps.
   - ❒ if you are using a 1 Mbps SpectraLink telephone, set it to 1 Mbps.

5. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

Configuring the 802.11a Radio

The 802.11a radio will communicate with other 802.11a radios that have the same:

- SSID (Network Name)
- Security

For each radio, you can assign up to four SSIDs, creating one primary service set and up to three secondary service sets. Each service set shares the same Advanced Configuration and Inbound Filters settings, but you can customize the security settings. However, most clients do not support a mixed security environment using multiple service sets:

- If you configure security on the primary service set, then you should also configure security on the secondary service sets.
- If you do not configure security on the primary service set, then you cannot configure security on the secondary service sets.

For details, see "When You Configure Different SSIDs with Different Security Settings" on page 172.

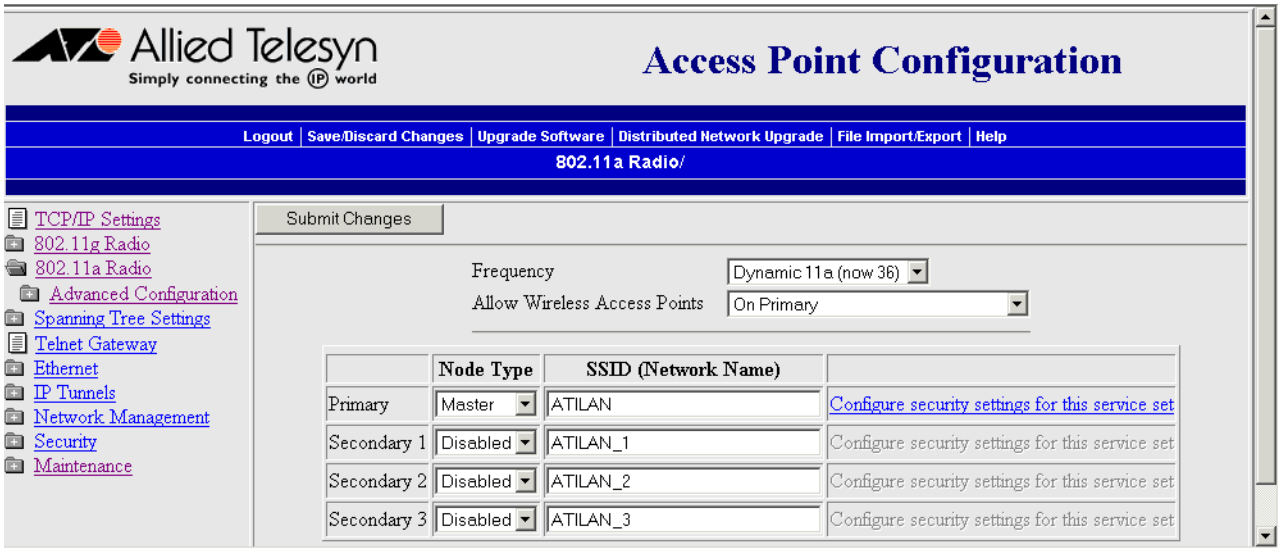
Multiple service sets are used primarily to allow one physical radio to support multiple virtual LANs (VLANs). For details about VLANs, see "Configuring VLANs" on page 187.

The 802.11a radio ships with either the full-range (5.15 to 5.35 GHz) option or the mid-range (5.25 to 5.35 GHz) option. The full-range option can only be used indoors and with the integrated antenna.

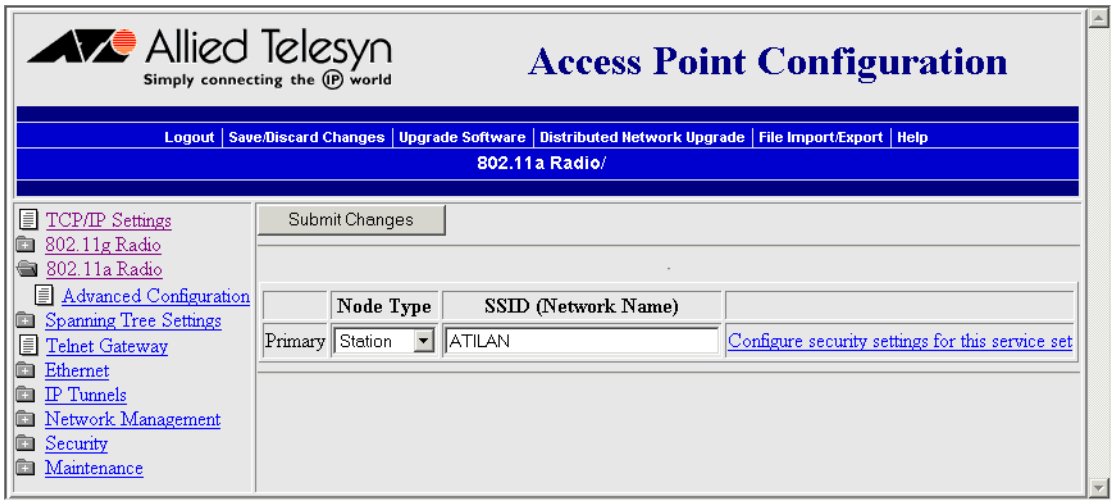
If you configure an 802.11a radio as a master radio, it provides simultaneous master and station support. This feature means that not only do you only need one radio in WAPs and point-to-multipoint bridges, but also it can "heal itself." If the access point can no longer communicate with the Ethernet network, it will try to wirelessly connect to the root through another access point. Any access point that may become a WAP should have a root priority set to 0 and have a secondary LAN bridge priority.

To configure the 802.11a radio

1. From the main menu, click 802.11a Radio. The 802.11a Radio screen appears.



If your screen does not look like the previous one, your primary service set may be configured as station (instead of master), so that the secondary service sets are not available, as shown next.



2. Configure the parameters for the radio. For help, see the next table.

3. Configure the advanced parameters for the radio. For help, see “Configuring 802.11a Radio Advanced Parameters” on page 124.

4. (Master only) Configure inbound filters. For help, see “Configuring 802.11a Radio Inbound Filters” on page 126.

5. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

6. (Optional) Configure security by clicking Configure security settings for this radio. For help, see Chapter 6, "Configuring Security" on page 169.

Table 37. 802.11a Radio Parameter Descriptions

Parameter	Explanation
Frequency (Master radio only)	Choose the frequency within the 5.15 to 5.35 GHz range that this access point uses to transmit and receive frames. You can also set the frequency to Dynamic, which lets the access point choose the best available channel to use. The available frequencies depend on the country and the radio option configured on the access point. See the Table 38, "Worldwide Frequencies for the 802.11a Radio" on page 123. If the radio is a mid range radio, you can only choose 52, 56, 60, or 64. You may want to use a single frequency to isolate the installation to part of the band; for example, use a single frequency if other wireless networks or microwave ovens are in the area.
Allow Wireless Access Points	Choose which service set provides connection for wireless access points: On Primary: The primary service set connects to wireless access points. On Secondary n: The secondary service set n (where n is 1, 2, or 3) connects to wireless access points. Do not allow wireless access points: No service set connects to wireless access points. You can block access points from forming a wireless hop to this radio entirely.

Table 37. 802.11a Radio Parameter Descriptions (Continued)

Parameter	Explanation
Node Type	Configure the 802.11a radio to master, station, or disabled: Master: The radio operates in Master mode when it sees the root access point on its Ethernet port. If it cannot see the root, it operates in Master/ Station mode and tries to find the root through its radio port. Station: The radio always operates in Station mode. Disabled: The radio is disabled. You can create up to four service sets for this radio by setting the Node Type field as follows: ❒ If the primary service set is Master, up to three secondary service sets may be set to Master. ❒ If the primary service set is Station, all secondary service sets are disabled and do not appear on screen. ❒ If the primary service set is Disabled, all secondary service sets (and the physical radio) are disabled.
SSID (Network Name)	Enter a unique SSID for each service set. You can enter up to four SSIDs for this radio. The SSID is case sensitive and cannot be more than 32 alphanumeric characters. 802.11a radios communicate with other 802.11a radios with the same SSID. You need to assign the same network name to the wireless end devices that will connect to the radio.

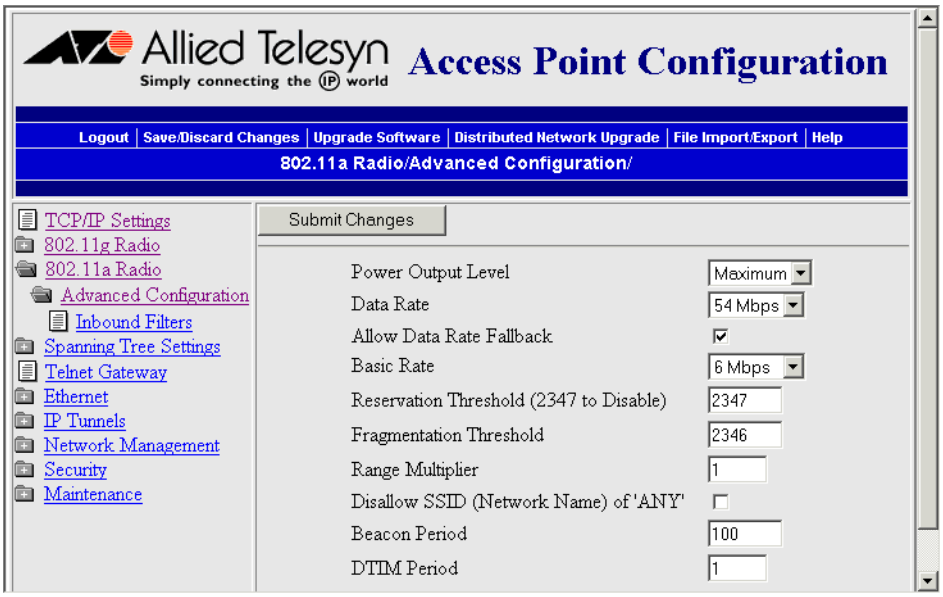
Table 38. Worldwide Frequencies for the 802.11a Radio

Channel	FCC	ETSI	France	Japan	Israel
36*	5180 (default)	N/A	N/A	N/A	N/A
40*	5200	N/A	N/A	N/A	N/A
42*	5210 Turbo	N/A	N/A	N/A	N/A
44*	5220	N/A	N/A	N/A	N/A
48*	5240	N/A	N/A	N/A	N/A
50*	5250 Turbo	N/A	N/A	N/A	N/A
52	5260 (default)	N/A	N/A	N/A	N/A
56	5280	N/A	N/A	N/A	N/A
58	5290 Turbo	N/A	N/A	N/A	N/A
60	5300	N/A	N/A	N/A	N/A
64	5320	N/A	N/A	N/A	N/A

- Channels marked with an asterisk (*) are not available in the mid-range radio.
- If you set the Frequency parameter to Dynamic, turbo channels are never selected.
- FCC countries include the United States, Canada, China, Taiwan, India, Thailand, Indonesia, Malaysia, Hong Kong, and most South American countries. The 802.11a channels that are allowed in a given country may change without notice. Be sure you use only those frequencies that are permissible in the given country.

Configuring 802.11a Radio Advanced Parameters

1. From the main menu, click 802.11a Radio > Advanced Configuration. The Advanced Configuration screen appears.



2. Configure the advanced parameters. For help, see the next table.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

Table 39. 802.11a Radio Advanced Parameter Descriptions

Parameter	Description
Power Output Level	Set the transmitted power level: Maximum: Sets the output power to the highest level supported by the radio. Medium: Sets the output power to a lower level than the highest level supported by the radio. Low: Sets the output power to a level higher than the lowest level supported by the radio. Minimum: Sets the output power to the lowest level supported by the radio. Lowering the power output level reduces the radio coverage for this area and reduces the range for this radio.

Table 39. 802.11a Radio Advanced Parameter Descriptions (Continued)

Parameter	Description
Data Rate	Choose the rate at which the access point transmits data. In general, higher speeds mean shorter range and lower speeds mean longer range. If you choose the Speed Mode to be 802.11 compliant, you can set this rate to 54, 48, 36, 24, 12, or 6 Mbps.
Allow Data Rate Fallback	Determines if you want the radio to drop to a slower data rate when it has trouble communicating with another radio. If this parameter is disabled, the Basic Rate parameter is not available because the basic rate becomes the same value as the Data Rate parameter.
Basic Rate	Appears only if the Allow Data Rate Fallback parameter is enabled. Choose the rate at which the access point transmits multicast and beacon frames. In general, higher speeds mean shorter range and lower speeds mean longer range. Do not set this rate higher than the maximum rate at which your end devices can receive multicast frames. You can set this rate to 24, 12, or 6 Mbps. This parameter should usually be left at the default of 6 Mbps.
Reservation Threshold	You may need to set a threshold value, which is the largest data frame that can be transmitted without reserving airtime. Airtime is normally reserved to help prevent collisions with other transmitters. If you set this threshold to 2347, this parameter is disabled.
Fragmentation Threshold	Specifies the largest data frame that can be transmitted without fragmentation. On certain radios, the fragmentation does not occur unless the radio detects interference. Larger frame sizes can improve throughput on a reliable connection. Smaller frame sizes can improve throughput on a poor connection.

Table 39. 802.11a Radio Advanced Parameter Descriptions (Continued)

Parameter	Description
Disallow SSID (Network Name) of 'ANY' (Master radio only)	Determines if end devices that have their SSID (Network Name) set to ANY or are left blank can associate with this access point. Clear this check box to allow these end devices to associate with this access point. Although this setting is 802.11 compliant, it is not very secure. Check this check box to prevent end devices with an SSID of ANY or are left blank from associating with this access point.
Beacon Period	Specifies how often the access point sends out a beacon frame. This rate is in TU. (A TU is 1024 ms and is often considered to be equivalent to 1 ms.)
DTIM Period	Specifies the number of beacon periods to skip before including a DTIM (delivery traffic indication message) in a beacon frame. Setting a higher DTIM period may conserve battery life in an end device, but it may increase response time.

Configuring 802.11a Radio Inbound Filters

When configuring a master radio, you can filter different types of wireless traffic that it may receive. You may want to use this feature by itself or with an access control list (ACL) to help secure your network. If you clear all the check boxes, the radio cannot communicate with any other radios.

You check the Allow IAPP check box so the access point can communicate with other access points and participate in the spanning tree.

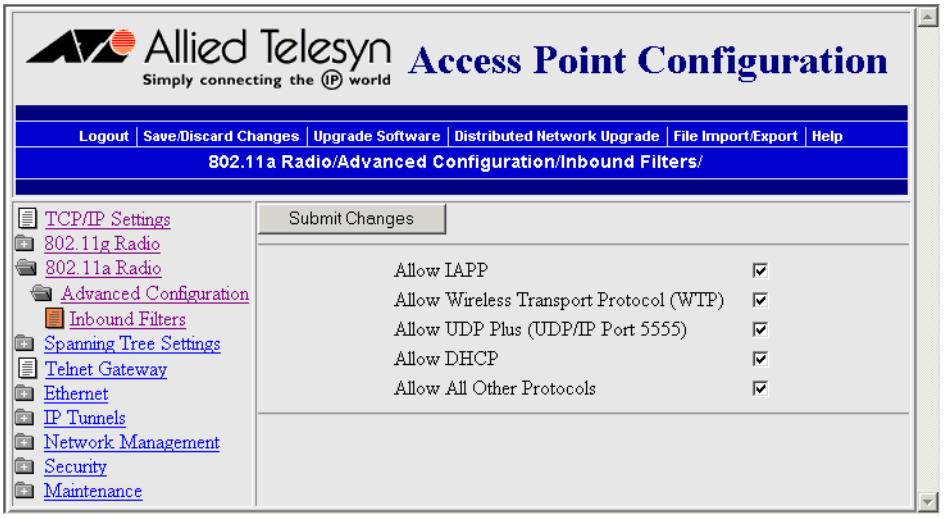
You can use this feature to form a secure wireless hop. Clear all check boxes, except for the Allow IAPP check box.

Or you may want to use this feature in a terminal emulation environment when you know the end devices are sending only UDP Plus or Wireless Transport Protocol (WTP) frames. Check the Allow UDP Plus check box or the Allow Wireless Transport Protocol check box and clear all other check boxes (except the Allow IAPP check box). The access point master radio will only accept the UDP Plus or WTP frames and discard all other frames, which can make a more secure network.

Note
If any of the devices are also DHCP clients, you need to check the Allow DHCP check box.

To configure 802.11a radio inbound filters

1. From the main menu, click 802.11a Radio > Inbound Filters. The Inbound Filters screen appears.



2. For each frame type, check or clear each check box. For help, see the next table.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Table 40. 802.11a Radio Inbound Filter Descriptions

Parameter	Description
Allow IAPP	Determines if this radio accepts IAPP (Inter Access Point Protocol) frames from other access point station radios. The IAPP frames must match Ethernet protocol 875c.
Allow Wireless Transport Protocol (WTP)	Determines if this radio accepts WTP frames from end devices. The WTP frames must match Ethernet protocol 875b.
Allow UDP Plus (UDP/IP Port 5555)	Determines if this radio accepts UDP Plus frames from end devices. The UDP Plus frames must match the UDP network port 5555 on the DCS 30X, Allied Telesyn Gateway, or ARP.

Table 40. 802.11a Radio Inbound Filter Descriptions (Continued)

Parameter	Description
Allow DHCP	Determines if this radio accepts DHCP frames. The DHCP frames must match UDP destination port 67 and ARP. Check this check box if the end devices are DHCP clients.
Allow All Other Protocols	Determines if this radio accepts all other protocols that are not filtered by one of the filters in this screen.
Multicast Filter	Determines if this radio can receive and send multicast frames.
File Name	Specifies the name of the radio's driver software. Allied Telesyn recommends that you change this name only when directed to do so by Allied Telesyn Technical Support.
Hello Period	Controls how frequently the access point broadcasts hello messages on this radio port. Hello messages help maintain the spanning tree and serve as beacon messages to synchronize communications with end devices.

Chapter 5

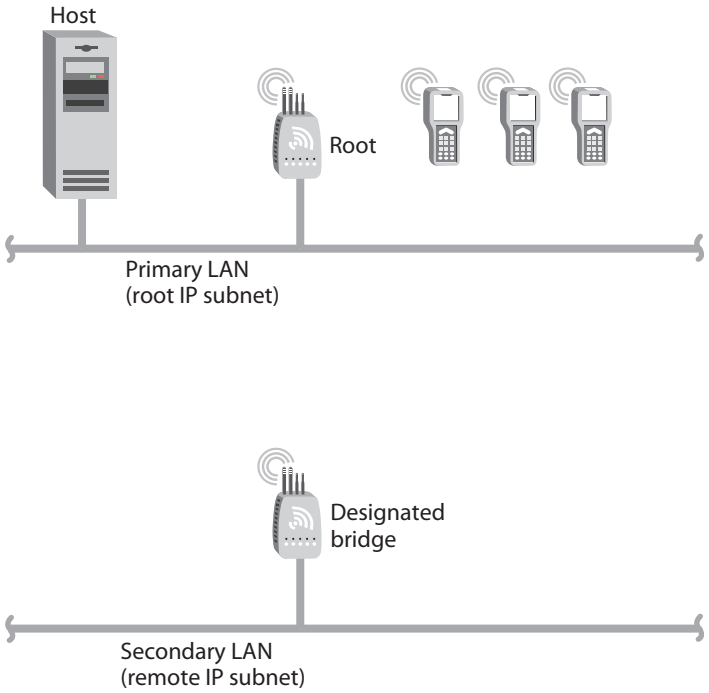
Configuring the Spanning Tree

This chapter explains how to configure the AT-WA7500 and AT-WA7501 access points so that they create a spanning tree topology. This chapter covers these topics:

About the Access Point Spanning Tree

AT-WA7500 and AT-WA7501 access points with the same LAN ID arrange themselves into a self-organized network using a spanning tree topology. The spanning tree provides efficient, loop-free forwarding of frames through the network and allows efficient roaming of wireless end devices. It contains at least a primary LAN and a root access point, but it may also contain secondary LANs, designated bridges, and other access points.

This spanning tree contains a root access point on the primary LAN and a designated bridge on the secondary LAN.



Within the spanning tree, access points use IAPP (Inter Access Point Protocol) or secure IAPP to communicate with each other across the Ethernet network, over wireless secondary LANs, and through IP tunnels to remote IP subnets. IAPP also enables fast roaming in an 802.11g, 802.11b or 802.11a network using 802.1x security. Secure IAPP prevents unauthorized access products from joining the spanning tree.

For example, when an end device roams to a new access point, the new access point informs the old access points via the root access point that any traffic for the end device needs to be routed to the new access point. As end devices are added to or removed from the network, access points are automatically updated so they can maintain reliable operation and communication.

About the Primary LAN and the Root Access Point

The primary LAN (also called the root IP subnet) contains the root access point, which initiates the spanning tree. When choosing the primary LAN, ideally you should choose the IP subnet that contains gateways or servers for the wireless end devices. However, these gateways and servers may also be on another subnet.

The root access point coordinates the network and distributes common system parameters to other access points and end devices. Consider these selection criteria when choosing which access point to be the root:

- The root must be installed on the primary LAN.
- The root should be an access point that does not handle a large volume of wireless traffic.
- Because the root distributes parameters to the child access points, the root should have the latest version of software available. In a mixed network of an AT-WA7500 or AT-WA7501 access point with AT-WL2411 access points, choose an AT-WA7500 or AT-WA7501 access point with software release 2.2 (or later) as the root.

The root is elected from a group of access points that are designated as root candidates: access points that are powered on, active, and do not have a root priority of 0. The access point with the highest root priority is the root. Root priority can range from 0 (off) to 7. The value 1 is the highest priority for a participating access point.

The election process also occurs in the event of a root access point failure. Besides the root, you should have two or three access points with a non-zero root priority. (Use the selection criteria listed earlier in this section to determine which access points should be root candidates.) If two access points have the same root priority, the access point with the highest Ethernet address becomes the root. You should configure your network with overlapping coverage so that the network can automatically recover from any single point of failure.

After the root access point is elected, it transmits hello messages on all enabled ports. The spanning tree forms as other access points receive hello messages and attach to the network on the optimal path to the root. A non-root access point also transmits hello messages after it is attached to the network. Each hello message contains the LAN ID of the access point that originated the message. IAPP does not allow wireless links to exist between access points that do not have matching LAN IDs.

To configure a root access point

1. Using the selection criteria listed earlier in this section, determine which access point to configure as the root.
2. On that access point, from the main menu click Spanning Tree Settings. The Spanning Tree Settings screen appears.

3. Configure the LAN ID. All access points that want to participate in the spanning tree must have the same LAN ID.
4. Set the Root Priority parameter to be the highest number of all access points on the primary LAN. Verify that the Enable Ethernet Bridging check box is checked. The range is 1 to 7. The value 1 is the highest priority.
5. Verify that the Secondary LAN Bridge Priority is zero.
6. Verify that the Secondary LAN Flooding parameter is Disabled.
7. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

About Secondary LANs and Designated Bridges

There are two types of secondary LANs:

- A wireless secondary LAN, which is an Ethernet segment containing access points that join the primary LAN network through a wireless connection
- A remote IP subnet, which is connected via an IP tunnel.

Table 41. Comparison of Wireless Secondary LANS and Remote IP Subnets

Wireless Secondary LANs	Remote IP Subnets
Any access point can provide a wireless link to another access point.	Only the root access point can originate an IP tunnel to another access point.
A wireless link provides a transparent bridge for both wired and wireless devices.	An IP tunnel provides a transparent bridge for wireless end devices on a remote IP subnet.

The access point that is responsible for bridging data between a secondary LAN and the primary LAN is called the designated bridge. Consider these selection criteria when choosing which access point to be the designated bridge:

- The designated bridge should have the latest version of software available. In a mixed network of AT-WA7500 and AT-WA7501 access points with AT-WL2411 access points, choose a AT-WA7500 or AT-WA7501 access point with software release 2.2 (or later) as the designated bridge.
- The designated bridge must be installed on the secondary LAN and within radio coverage of an access point on the primary LAN.

- The designated bridge must be configured so that the Secondary LAN Bridge Priority value is a non-zero number.
- The designated bridge must have at least one radio set to Station mode, or the designated bridge must be the endpoint of an IP tunnel (as defined in "About IP Tunnels" on page 140).

If more than one access point meets these requirements, the access point with the highest secondary LAN bridge priority is the designated bridge. If two access points have the same secondary LAN bridge priority, the access point with the highest Ethernet address becomes the designated bridge. If the designated bridge goes offline, the remaining access points negotiate to determine which access point becomes the new designated bridge.

To configure a designated bridge

1. Using the selection criteria listed earlier in this section, determine which access point to configure as the designated bridge.
2. On that access point, from the main menu click Spanning Tree Settings. The Spanning Tree Settings screen appears.
3. Configure the LAN ID. All access points that want to participate in the spanning tree must have the same LAN ID.
4. Set the Root Priority parameter to zero. All access points on the secondary LAN should have a root priority of zero.
5. Verify that the Enable Ethernet Bridging check box is checked.
6. Set the Secondary LAN Bridge Priority to be the highest number of all access points on the secondary LAN. The range is 1 to 7. The value 1 is the highest priority.
7. Set the Secondary LAN Flooding parameter to Enabled.
8. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

About Ethernet Bridging/Data Link Tunneling

Ethernet bridging is simply forwarding a frame received on the radio port to the Ethernet port, and vice versa. Using this default mode, the access point acts as a bridge between the wireless and wired networks.

> **Note**
> Allied Telesyn recommends that you enable Ethernet bridging on all access points. However, if you meet the criteria listed later in this section, you can disable Ethernet bridging and use data link tunneling instead. Be aware that data link tunneling increases network traffic.

Turning off Ethernet bridging enables data link tunneling. The data link tunneling mode causes the child access point to encapsulate inbound wireless data into an 875C frame. This data frame is then forwarded via the Ethernet port to the next access point on the path, and so on, until the frame reaches the root access point or designated bridge. The root access point or designated bridge encapsulates the frame and forwards it to the host. When the root access point or designated bridge receives data on the Ethernet network for an end device, it reverses this process.

When should you use data link tunneling?

- Use data link tunneling if you have Ethernet switches that do not support the IEEE 802.1d requirements for backward learning. Some proprietary VLAN switches and ATM LANE bridges do not support this standard.

  If the access points are connected to different ports on an Ethernet switch, each time an end device roams to a new access point, it appears on a different port. Thus, frames sent to the end device from the host are sent to the wrong port. If the switch does not support 802.1d, it may become confused and communications with the end device are disrupted. Data link tunneling makes end device roaming transparent to the switch. All the information appears to originate from only one port on the switch–the port that is connected to the root access point or designated bridge.

- Use data link tunneling when you are using IP tunnels to provide mobility of other routable protocols, such as IPX. In some network installations, detecting these addresses may generate alarms or cause switches to behave erroneously. In this situation, using data link tunneling does not increase network traffic.

To enable data link tunneling on the primary LAN

1. Make sure that all access points have the same LAN ID.
2. On the root access point, on the Spanning Tree Settings screen verify that the Enable Ethernet Bridging check box is checked.

3. On all other access points on the primary LAN, clear the Enable Ethernet Bridging check box.

4. Make sure that the Root Priority parameter for all other access points is less than the root access point. The range is 1 to 7. The value 1 is the highest priority.

To enable data link tunneling on the secondary LAN

1. Make sure that all access points have the same LAN ID as the ones on the primary LAN.

2. On the designated bridge, on the Spanning Tree Settings screen verify that the Enable Ethernet Bridging check box is checked.

3. On all other access points on the secondary LAN, clear the Enable Ethernet Bridging check box.

4. Make sure that the Secondary LAN Bridge Priority parameter for all other access points is less than the designated bridge.

If you use data link tunneling on the secondary LAN and end devices have IP addresses on the secondary LAN, network monitoring tools and other network components cannot detect their MAC/IP addresses. For more information, see "About IP Tunnels" on page 140.

About Routable and Non-Routable Network Protocols

Hosts that use a routable network protocol such as IP or IPX may be located on any IP subnet; however, triangular routing can be minimized if servers are located on the root IP subnet. (Note that this is also true for standard mobile IP.) You should be able to use default flooding and spanning tree settings if you are using routable protocols, even if hosts are located on remote IP subnets.

Configuring the Spanning Tree Parameters

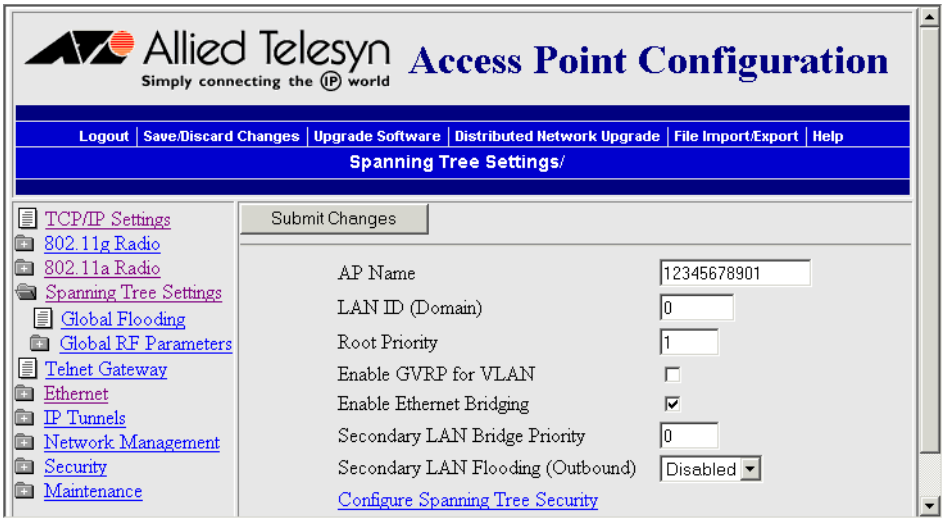
When you configure the spanning tree parameters, you identify the access point as part of the spanning tree. That is, you specify if this access point is a root, or a candidate to become a root, or a designated bridge, or a candidate to become a designated bridge.

You also specify if the access point uses Ethernet bridging to forward frames between the wired and wireless networks. Allied Telesyn recommends that you use Ethernet bridging on all access points unless you meet the criteria listed in “About Ethernet Bridging/Data Link Tunneling” on page 134.

Note
On the designated bridge, if you disable Ethernet bridging or if you set the Secondary LAN Bridge Priority to 0, wireless traffic is encapsulated on the secondary LAN, which eliminates communication from wired devices on the secondary LAN.

To configure the spanning tree parameters

1. From the main menu, click Spanning Tree Settings. The Spanning Tree Settings screen appears.



2. Configure the spanning tree parameters. For help, see the next table.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

4. (Optional) Configure security by clicking Configure Spanning Tree Security. For help, see "Creating a Secure Spanning Tree" on page 181.

Table 42. Spanning Tree Parameter Descriptions

Parameter	Explanation
AP Name	Enter a unique name for this access point. The name can be from 1 to 16 characters. The default is the access point serial number.
LAN ID (Domain)	Enter the LAN ID. All access points must have the same LAN ID to participate in the same spanning tree. The LAN ID is a number from 0 to 254.
Root Priority	Determines if this access point is a candidate to become the root of the spanning tree. The access point with the highest root priority becomes the root whenever it is powered on and active. The root priority can be a value from 0 (off) to 7. The value 1 is the highest priority for a participating access point. If you set the root priority to 0, the access point can never become the root access point. All access points on the secondary LAN should have a root priority of 0. For help deciding if this access point should be a candidate to become root, see "About the Primary LAN and the Root Access Point" on page 131.
Enable GVRP for VLAN	The access point uses GARP VLAN Registration Protocol (GVRP) to request a VLAN-capable Ethernet switch to forward traffic for specific VLANs. Enabling this parameter lets the switch exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast, prune unknown unicast traffic, and dynamically create and manage VLANs on switches connected through 802.1Q trunk ports. A switch may also be configured statically to always forward specific VLANs to specific ports. You should clear this check box for a static configuration.

Table 42. Spanning Tree Parameter Descriptions (Continued)

Parameter	Explanation
Rightmost LED Behavior	Choosing Spanning Tree Root Indicator causes the LED to blink if the access point is configured as the root and remain on if an error is detected.
Enable Ethernet Bridging	Determines how frames from end devices are moved between the wired and wireless networks. For more details, see “About Ethernet Bridging/ Data Link Tunneling” on page 134. Check this check box if you want frames to be forwarded directly to the Ethernet network. Allied Telesyn recommends that you enable this parameter on all access points. Clear this check box if you meet the selection criteria listed in “About Ethernet Bridging/Data Link Tunneling” on page 134 and you want to use data link tunneling. **Note** If you enable this parameter on the root or designated bridge, but you disable it on all other access points on the same IP subnet, then Ethernet bridging is disabled on the IP subnet. This means that data link tunneling is enabled on the IP subnet.
Secondary LAN Bridge Priority	Determines when this access point can become the designated bridge in a secondary LAN. The access point that meets all the other requirements and has the highest secondary LAN bridge priority becomes the designated bridge. The secondary LAN bridge priority can be a value from 0 to 7. If you set this value to 0, the access point can never become the designated bridge. For help deciding if this access point should become the designated bridge, see the selection criteria listed in “About Secondary LANs and Designated Bridges” on page 132.

Table 42. Spanning Tree Parameter Descriptions (Continued)

Parameter	Explanation
Secondary LAN Flooding (Outbound)	Appears for Designated Bridge only. Specifies the types of frames it forwards from the primary LAN to the secondary LAN: Disabled: No flooding occurs unless the root access point (in the Global Flooding screen) enables the Multicast or Unicast Outbound to Secondary LANs parameter. Enabled: Multicast and unicast flooding occurs unless the root access point (in the Global Flooding screen) disables multicast or unicast flooding. Multicast: Multicast flooding occurs unless the root access point (in the Global Flooding screen) disables multicast flooding. Unicast: Unicast flooding occurs unless the root access point (in the Global Flooding screen) disables unicast flooding.

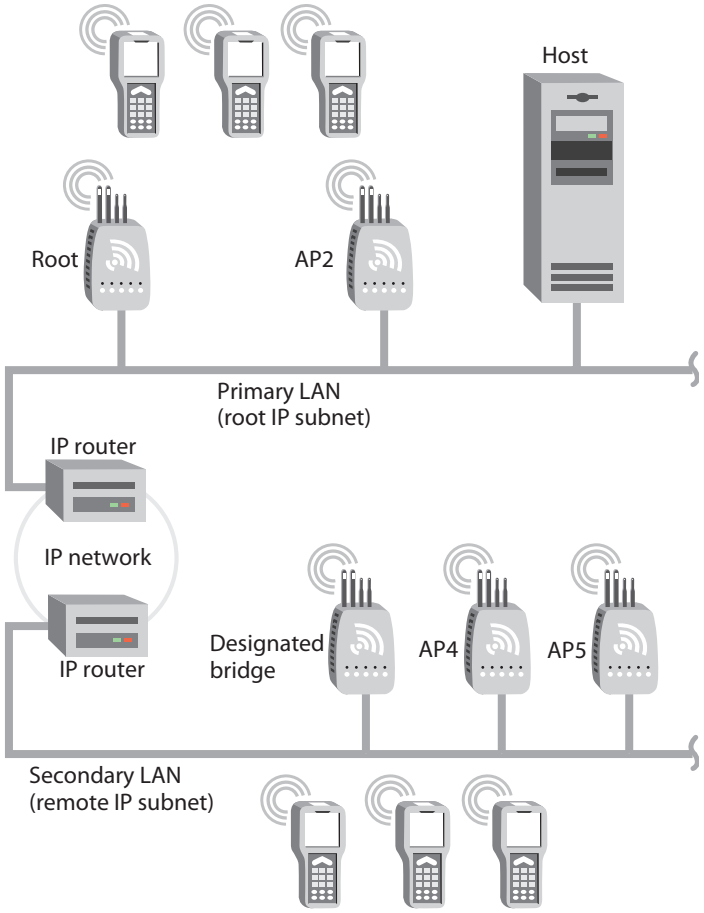
About IP Tunnels

The physical boundary of a network is usually defined by the existence of an IP router. Before IP tunnels technology was developed, wireless end devices could only operate within the limited coverage area of their own network and could not roam across IP subnet boundaries. Using IP tunnel technology, end devices can roam across IP subnet boundaries. IP tunnel technology safely and transparently coexists with routed IP installations while supporting mobility for end devices.

IP tunnels do the following:

- Enable access points on different remote IP subnets to belong to the same wireless network.
- Support fast roaming of end devices between access points that are on different IP subnets without losing network connections.
- Support end devices using both IP and other routable or nonroutable protocols.

Only one IP tunnel can exist between the root access point and an access point (usually the designated bridge) on a remote IP subnet. The root access point has a one-to-one relationship with each wireless network. All roaming end devices must have an IP address from the root IP subnet.



IP tunnels use encapsulation to establish a virtual LAN (VLAN) segment through IP routers. The VLAN segment includes the root IP subnet and logically extends to include end devices attached to access points on remote IP subnets. IP tunnels are branches in the spanning tree topology.

Any access point on a secondary LAN that can receive IP hello messages can be the endpoint of an IP tunnel. Usually, the access point that is the endpoint of an IP tunnel is also the designated bridge. After an IP tunnel is formed between the root access point and an access point on a remote IP subnet, end devices can roam to the remote IP subnet. End devices must have an IP address from the root IP subnet. However, there are no address restrictions for non-IP end devices. When end devices roam to the remote IP subnet, their data is IP tunneled back to the root IP subnet (where it belongs) and everything works properly.

If you have a DHCP server in your network, it must be on the root IP subnet. All access points on secondary LANs must have permanent IP addresses. On the root access point, you must allow IP multicast frames to pass.

When an access point at the endpoint of the IP tunnel receives data from an end device, it uses a standard IP protocol called Generic Router Encapsulation (GRE) to encapsulate the data into a frame. These encapsulated IP/GRE frames use normal IP routing to pass through IP routers to the root access point. The root access point unencapsulates the frame and forwards it to the host. When the root access point receives data on the Ethernet network for an end device that is communicating on a remote IP subnet, it reverses this process.

IP tunneling also allows non-routable traffic, such as WTP and NNL, to roam across routers. The end devices using these protocols are not IP based, but they work in the same way. Data traffic that is not passed by routers (since they are not IP) will be tunneled from the remote IP subnet to the root subnet. It will be dumped on the Ethernet on the root subnet (where it belongs) and everything works properly.

Creating IP Tunnels

An IP tunnel is established when an access point on a remote IP subnet attaches to the root access point through its IP tunnel port. The number of IP tunnels the root access point can originate is practically unlimited. However, currently the IP address list can only contain eight entries, which effectively limits the number of tunnels that can be created if you want to use unicast and directed broadcast IP addresses.

The IP address list can contain any combination of IP unicast, IP broadcast, or IP multicast addresses:

- Only one IP tunnel can be created for each IP unicast address in the list.
- One IP directed broadcast address can be used to create a practically unlimited number of tunnels to a single remote IP subnet. (An IP directed broadcast address is typically used to specify all hosts on a single remote subnet.)
- One IP multicast address can be used to create a practically unlimited number of tunnels to remote IP subnets. For help, see “Using One IP Multicast Address for Multiple IP Tunnels” on page 144.

Once you have configured the IP tunnels, the root access point sends IP hello messages to each IP address in its IP address list. An IP tunnel is automatically established when an access point on a remote IP subnet receives this hello message. This access point then transmits IP hello messages on its subnet so that other access points on the same subnet that do not receive hello messages can also attach to the spanning tree.

To create a unicast IP tunnel

1. Make sure that end devices that will roam between the root IP subnet and the remote IP subnet have IP addresses from the root IP subnet and have their default router set the same as the root access point. There are no address restrictions for non-IP end devices.

2. Make sure that the root access point and the access point at the endpoint of the IP tunnel have the same LAN ID.

3. On the root access point, set the Mode parameter to Originate if Root. For help configuring a root access point, see "About the Primary LAN and the Root Access Point" on page 131.

4. On the access point at the endpoint of the IP tunnel, set the Mode parameter to Listen.

5. On the root access point, click IP Tunnels > IP Addresses. Enter the IP address or DNS name of the access point at the endpoint of the IP tunnel.

6. On the root access point and the access point at the endpoint of the IP tunnel, click Frame Type Filters. If you have end devices communicating using IP, set these DIX filters to Pass:

   - ❒ DIX-IP-TCP Ports
   - ❒ DIX-IP-UDP Ports
   - ❒ DIX-IP-Other Protocols
   - ❒ DIX-IPX Sockets
   - ❒ DIX-Other EtherTypes

7. On the root access point and the access point at the endpoint of the IP tunnel, click Predefined Subtype Filters.

   If you have end devices communicating using IP, set these filters to Pass:

   - ❒ DIX ARP
   - ❒ ICMP

8. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Using One IP Multicast Address for Multiple IP Tunnels

IP tunneling supports IP multicast and Internet Group Management Protocol (IGMP). IP multicast provides an ideal way to distribute IP hello messages. These hello messages are only forwarded to those IP subnets and IP hosts (such as access points) that participate in the multicast group. IP multicast has these advantages:

- You do not have to know the unicast or directed broadcast IP addresses in advance.
- IP multicast provides better built-in redundancy than IP unicast, because any access point can establish an IP tunnel.

IGMP is a standard protocol that lets you originate multiple IP tunnels using one IP multicast address. It allows IP multicast frames to be routed to remote IP subnets that have hosts participating in the multicast group. Note that IGMP is independent of IP; it can be used to facilitate multicast for IP or any other application. IGMP has these advantages:

- Causes IP hello messages to be forwarded only to those subnets that participate in the IP multicast group
- Increases redundancy because multiple access points on a remote subnet can receive IP hello messages

IP routers only forward multicast frames to those subnets that have IP hosts that participate in the respective IP multicast group. An IP host uses IGMP to notify IP routers that it wants to participate in an IP multicast group.

Access points can act as IP hosts and participate in an IP multicast group by enabling IGMP. The Internet Assigned Numbers Authority has allocated 224.0.1.65 for the AT-WA750x's IAPP. You must enter this address in the IP address list in the root access point (the address list may contain other IP addresses) and in the Multicast Address field in the other access points.

If you enable IGMP on the root access point, the root access point uses a Class D IP multicast address to send IP hello messages through IP routers to access points on other subnets. If you enable IGMP on remote IP subnets, intermediate IP routers will forward the IP hello messages to those subnets. Normally, you should enable IGMP and configure the IP multicast address in at least one access point on each remote IP subnet. (Some routers can provide proxy IGMP services for IP hosts.)

To create a multicast IP tunnel

1. Make sure that end devices that will roam between the root IP subnet and the remote IP subnet have IP addresses from the root IP subnet and their default router is set the same as the root access point. There are no address restrictions for non-IP end devices.

2. Make sure that your routers are configured to pass multicast frames.

3. Make sure that the root access point and the access point at the endpoint of the IP tunnel have the same LAN ID.

4. On the root access point, set the Mode parameter to Originate if Root. For help configuring a root access point, see "About the Primary LAN and the Root Access Point" on page 131.

5. On the access point at the endpoint of the IP tunnel, set the Mode parameter to Listen.

6. On the root access point, click IP Tunnels > IP Addresses. Enter the Allied Telesyn multicast address 224.0.1.65.

7. On the access point at the end of the IP tunnel, check the Enable IGMP check box.

8. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

How Frames Are Forwarded Through IP Tunnels

The access point maintains a forwarding database of all MAC addresses, and it knows the correct port for each MAC address. The access point updates this database by monitoring source addresses on each port (backward learning), by receiving explicit attachment messages, and by examining messages exchanged between access points when end devices roam. The database also includes the power management status of each end device, which allows the access point to support the pending message feature of the network. The forwarding database allows the Ethernet bridging software to make efficient forwarding decisions.

Any frame that is sent through an IP tunnel is addressed to the unicast IP address of the access point at the other end of the tunnel. An access point at the remote end of the tunnel learns the unicast IP address of the root access point by listening to IP hello messages. The root access point learns the unicast IP address of a remote access point when the access point attaches to the network.

Outbound Frames

Frames are forwarded outbound (to a secondary LAN) through an IP tunnel if:

- an end device is known to be attached to an access point on a remote IP subnet.
- the frame type is configured to pass.

IP and ARP frames are never forwarded outbound through an IP tunnel unless the destination IP address belongs to the root IP subnet. Usually, these frames are destined for wireless end devices that have roamed

away from their root IP subnet.

Unicast frames are not flooded. Unicast frames are only forwarded outbound through an IP tunnel if the destination address identifies an end device that has roamed to a remote IP subnet. End devices attach to the root access point, which maintains entries for these devices in its forwarding database. The database entries indicate the correct subnet for outbound forwarding.

For TCP/IP applications, IP and ARP frames must be forwarded through IP tunnels. An IP or ARP frame is only forwarded outbound if the destination address identifies an end device on the root IP subnet. Usually, ARP requests (which are multicast frames) that originate on the root IP subnet are forwarded outbound to all devices on the network, including through IP tunnels to remote IP subnets. However, if you enable ARP flooding, ARP frames are only sent through the IP tunnel to the destination end device.

MAC frames that are forwarded outbound are encapsulated in the root access point, forwarded through the network, unencapsulated by the access point at the remote end of the IP tunnel, and forwarded to the appropriate access point (if necessary) for delivery to the destination end device.

Inbound Frames

Frames are forwarded inbound (to the primary LAN) through an IP tunnel if:

- an end device is known to be attached to an access point on a remote IP subnet.
- the frame type is configured to pass.

IP and ARP frames are only forwarded inbound through the IP tunnel if the source IP address belongs to the root IP subnet. Usually, these frames originate from wireless end devices that have roamed away from their root IP subnet. Frames transmitted by servers or wired devices that are connected to a remote IP subnet are not forwarded inbound through IP tunnels if the IP address does not belong to the root IP subnet.

MAC frames that are forwarded inbound are encapsulated by the access point at the remote end of the IP tunnel, forwarded through the IP tunnel to the root access point, unencapsulated, and placed on the network.

Frame Types That Are Never Forwarded

Certain frame types are never forwarded through IP tunnels. Frame types that are never forwarded include IP frames used for coordinating routers and MAC frames used for coordinating bridges. Other frame types that are never forwarded include:

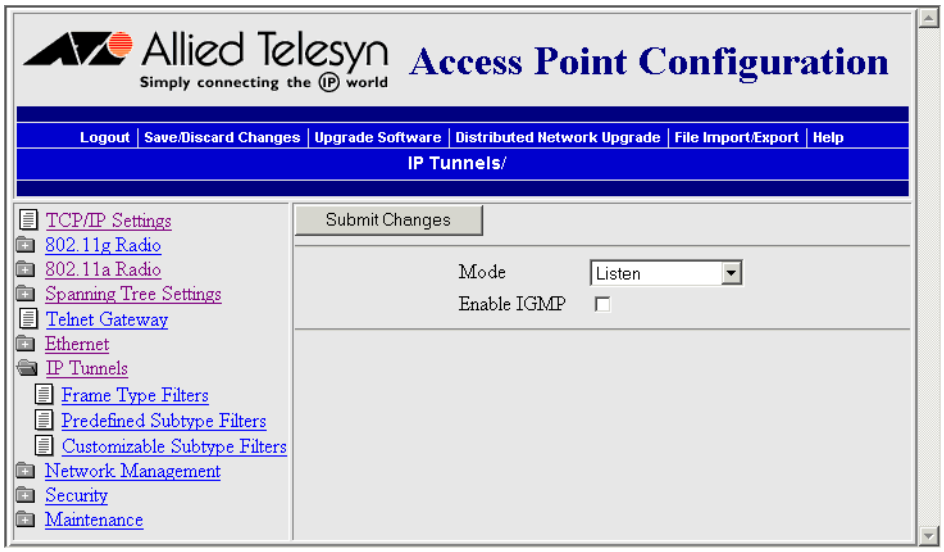
- 802.1d bridge frames
- Proprietary VLAN switch frames
- IP frames with a broadcast or multicast Ethernet address
- IP frames with the following router protocol types and decimal values:
  - DGP (86) (Dissimilar Gateway Protocol)
  - EGP (8) (Exterior Gateway Protocol)
  - IDPR (35) (Inter-Domain Policy Routing Protocol)
  - IDRP (45) (Inter-Domain Routing Protocol)
  - IGP (9) (Interior Gateway Protocol)
  - IGRP (88)
  - MHRP (48) (Mobile Host Routing Protocol)
  - OSPFIGP (89) (Open Shortest Path First Interior Gateway Protocol)
- IP ICMP (Internet Control Message Protocol) types:
  - IPv6
  - Mobile IP
  - Router Advertisement
  - Router Selection
- IP/UDP (User Datagram Protocol) frames with the following destination protocol port numbers:
  - BGP (179) (Border Gateway Protocol)
  - RAP (38) (Route Access Protocol)
  - RIP (520) (Routing Information Protocol)
- IP/TCP frames with the following destination or source protocol port numbers:
  - BGP (179) (Border Gateway Protocol)
  - RAP (38) (Route Access Protocol)

Configuring IP Tunnels

For guidelines, see “About IP Tunnels” on page 140.

To configure the IP Tunnels screen

1. From the main menu, click IP Tunnels. The IP Tunnels screen appears.



2. Configure the IP tunnels parameters. For help, see the next table.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

Table 43. IP Tunnel Parameter Descriptions

Parameter	Explanation
Mode	Choose the mode: Originate if Root: Lets the root access point and root candidates originate the IP tunnel if they are functioning as the root access point for the network. Listen: Configures access points that are designated bridges or designated bridge candidates for their remote IP subnets to serve as the endpoint of an IP tunnel. Disabled: Disables the IP tunnel port.

Table 43. IP Tunnel Parameter Descriptions (Continued)

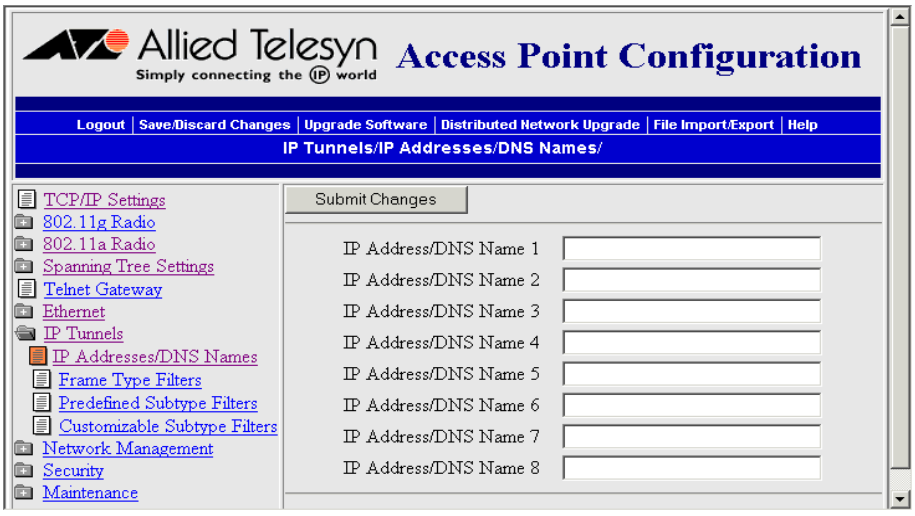
Parameter	Explanation
Allow IP Multicast	Appears only if Mode parameter is Originate if Root. Determines if the root access point should forward IP multicast frames through its IP tunnels. Check this check box if you have a DHCP server issuing TCP/IP information to end devices.
Enable IGMP	Appears only if Mode parameter is Listen. Determines if IGMP is enabled or disabled.
Multicast Address	Appears only if Enable IGMP check box is checked. Enter the Class D IP multicast address. You also need to enter this IP address in the root access point's IP address list. The Internet Assigned Numbers Authority has allocated 224.0.1.65 for Allied Telesyn's inter-access-point protocol (IAPP).

Configuring the IP Address List

On the root access point and root candidates, the IP address list contains the IP addresses or DNS names of all the access points at the endpoint of the IP tunnels. You can only configure this list if you set the Mode field to Originate If Root.

To configure the IP address list

1. From the main menu, click IP Tunnels > IP Addresses/DNS Names. The IP Addresses/DNS Names screen appears.



2. If you enabled IGMP, enter the Class D IP multicast address. The default is 224.0.1.65.

3. Enter the IP addresses or DNS names of all the access points that can be the endpoints of IP tunnels.

4. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

Configuring IP Tunnel Filters

You can set both Ethernet and IP tunnel filters, and you can create protocol filters for predefined protocol types. In addition, you can define arbitrary frame filters based on frame content.

By default, all IP tunnel traffic (except NNL traffic) is dropped. IP tunnel filters are only outbound filters. That is, when you configure IP tunnel filters in the root access point, you are only defining what type of traffic the root will send through the tunnel. The root will receive anything sent to it by the access point at the endpoint of the tunnel. The access point at the endpoint of the tunnel acts the same way. In order for a particular type of traffic to pass, you need to set the same filters to pass in both in the root access point and in the access point at the endpoint of a tunnel.

For help configuring Ethernet filters, see “Configuring Ethernet Filters” on page 80.

Using IP Tunnel Frame Type Filters

The IP tunnel port automatically provides some filtering for wireless end devices. You can define permanent IP tunnel port filters to prevent unwanted frame forwarding through an IP tunnel. ICMP frames with the following types are always forwarded:

- ❒ Echo Request
- ❒ Echo Reply
- ❒ Destination Unreachable
- ❒ Source Quench
- ❒ Redirect
- ❒ Alternate Host Address
- ❒ Time Exceeded
- ❒ Parameter Problem
- ❒ Time Stamp
- ❒ Time Stamp Reply
- ❒ Address Mask Request
- ❒ Address Mask Reply
- ❒ Trace Route

IP and ARP frames are never forwarded inbound through an IP tunnel to the root IP subnet unless the source IP address belongs to the root IP subnet. (Frames are only forwarded inbound if the source IP address in the IP or ARP frame identifies an end device that has roamed away from its root IP subnet.) IP and ARP frames are never forwarded outbound

through an IP tunnel by the root access point unless the destination IP address belongs to the root IP subnet. (Frames are only forwarded outbound to end devices that have roamed away from the root IP subnet.) For detailed information about other frame types that are never forwarded, see "Frame Types That Are Never Forwarded" on page 147.

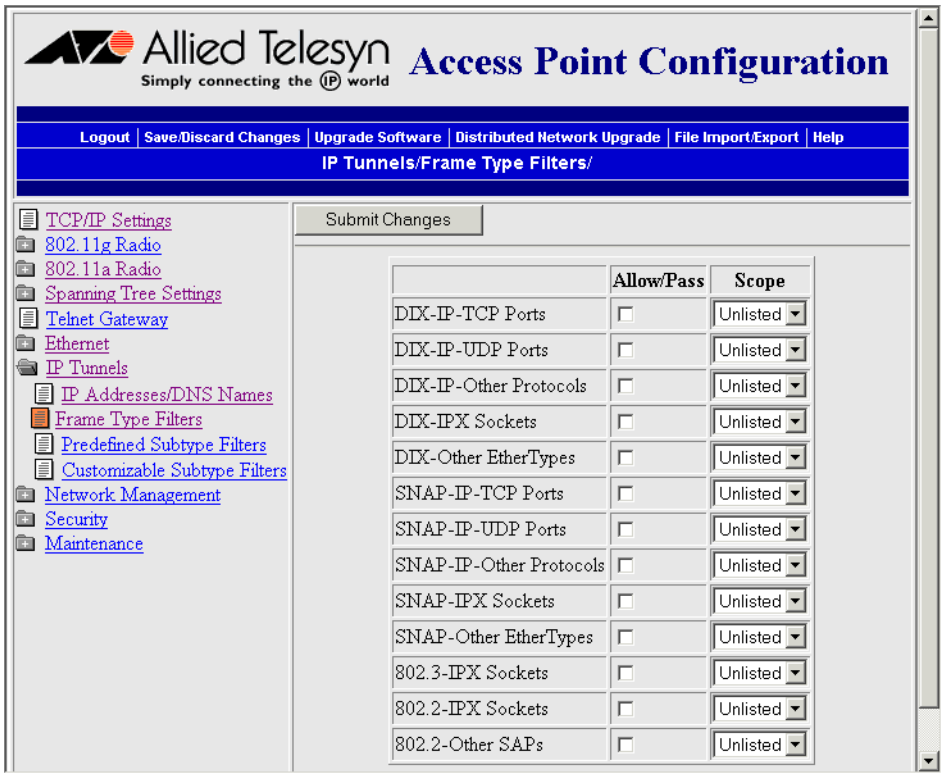
You can set the default action and scope for general and specific frame types:

Allow/ Pass: Check or clear this check box. Check this check box to pass all frames of the type. Clear this check box to drop all frames of the type.

Scope: Set scope to Unlisted or All. If you select All, then all frames of that type are unconditionally passed or dropped, depending on the action you specified. If you select Unlisted, then frames are passed or dropped only if the frame type is not listed in the predefined or customizable tables.

To use IP tunnel frame type filters

1. From the main menu, click IP Tunnels > Frame Type Filters. The Frame Type Filters screen appears.



2. For each frame type field, check or clear the check box to configure if the frame types are passed or are dropped. If you check the check box, the frame type is allowed to pass.

   For each frame type field, set the Scope field to Unlisted or All. For help, see the next table.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

4. If you set the Scope field to Unlisted for any of the frame types, you must also configure predefined subtype filters or customizable subtype filters. For help, see “Using Predefined Subtype Filters” on page 153 or “Customizing Subtype Filters” on page 153.

Table 44. Frame Type Filter Descriptions

Frame Type	Explanation
DIX IP TCP Ports DIX IP UDP Ports SNAP IP TCP Ports SNAP IP UDP Ports	Primary Internet Protocol Suite (IP) transport protocols.
DIX IP Other Protocols SNAP IP Other Protocols	IP protocols other than TCP or User Datagram Protocol (UDP).
DIX IPX Sockets	Novell NetWare protocol over Ethernet II frames.
SNAP IPX Sockets	Novell NetWare protocol over 802.2 SNAP frames.
802.3 IPX Sockets	Novell NetWare protocol over 802.3 RAW frames.
DIX Other Ethernet Types SNAP Other Ethernet Types	DIX or SNAP registered protocols other than IP or IPX.
802.2 IPX Sockets	Novell running over 802.2 Logical Link Control (LLC).
802.2 Other SAPs	802.2 SAPs other than IPX or SNAP.

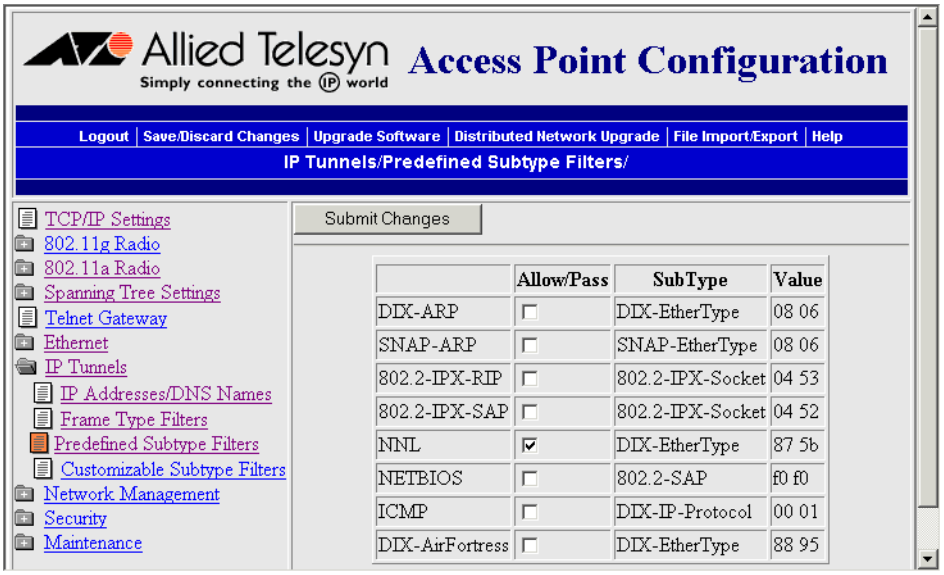
Note
You should not filter HTTP, Telnet, SNMP, and ICMP frames if you are using IP tunnels, because these filters are used for configuring, troubleshooting, and upgrading access points.

Using Predefined Subtype Filters

You can configure the access point to pass or drop certain predefined frame subtypes.

To configure predefined subtype filters

1. From the main menu, click IP Tunnels > Predefined Subtype Filters. The Predefined Subtype Filters screen appears.



2. For each frame subtype field, check or clear the check box to configure if the frame subtypes are passed or are dropped. If you check the check box, the frame subtype is allowed to pass.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Customizing Subtype Filters

You can define output filters that restrict customized frame subtypes that can pass through an IP tunnel. Frames can be filtered by the DIX, 802.2, or 802.3 SNAP type; the IP protocol type; or the TCP or UDP port number. By default, the filters drop all protocol types except the NNL DIX Ethernet type (hexadecimal 875B). Filters must be configured in all root candidates and in any access point that can attach to the remote end of an IP tunnel.

You define the action, subtype, and value parameters in customized filters:

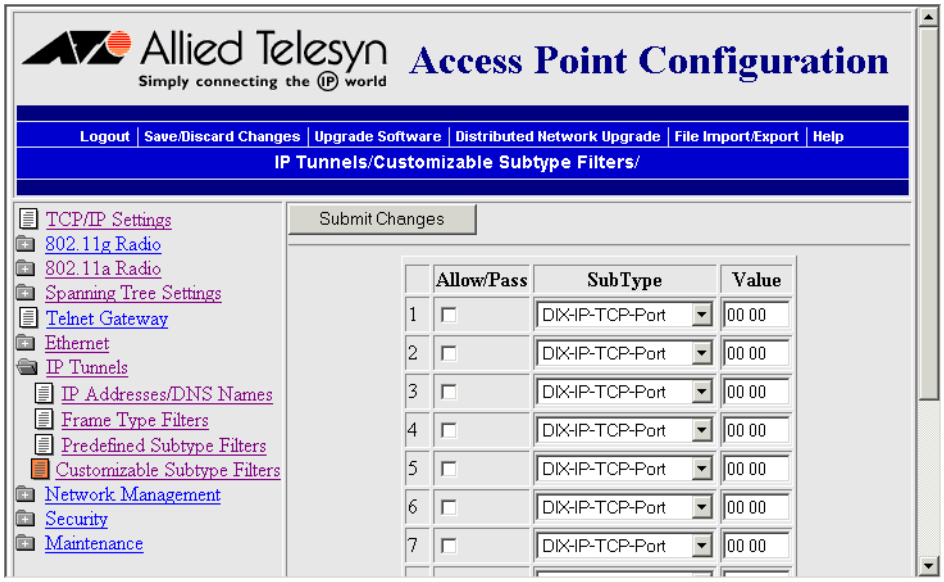
Allow/Pass: Check or clear this check box. Check this check box to pass all frames of the subtype and value. Clear this check box to drop all frames of the subtype and value.

Subtype: Selects the frame subtype you wish to configure.

Value: The next table describes frame subtypes and their values. The value must be two hex pairs. When a match is found between frame subtype and value, the specified action is taken.

To customize subtype filters

1. From the main menu, click IP Tunnels > Customizable Subtype Filters. The Customizable Subtype Filters screen appears.



2. For each frame subtype field, check or clear the Allow/Pass check box to configure if the frame subtypes are passed or are dropped. If you check the check box, the frame subtype is allowed to pass.

3. In the SubType field, choose the customizable frame subtype. For help, see the next table.

4. In the Value field, enter the two hex pairs. For help, see the next table.

5. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

Table 45. Subtype Filter Descriptions

Subtype	Value
DIX-IP-TCP-Port	Port value in hexadecimal.
DIX-IP-UDP-Port	Port value in hexadecimal.
DIX-IP-Protocol	Protocol number in hexadecimal.

Table 45. Subtype Filter Descriptions (Continued)

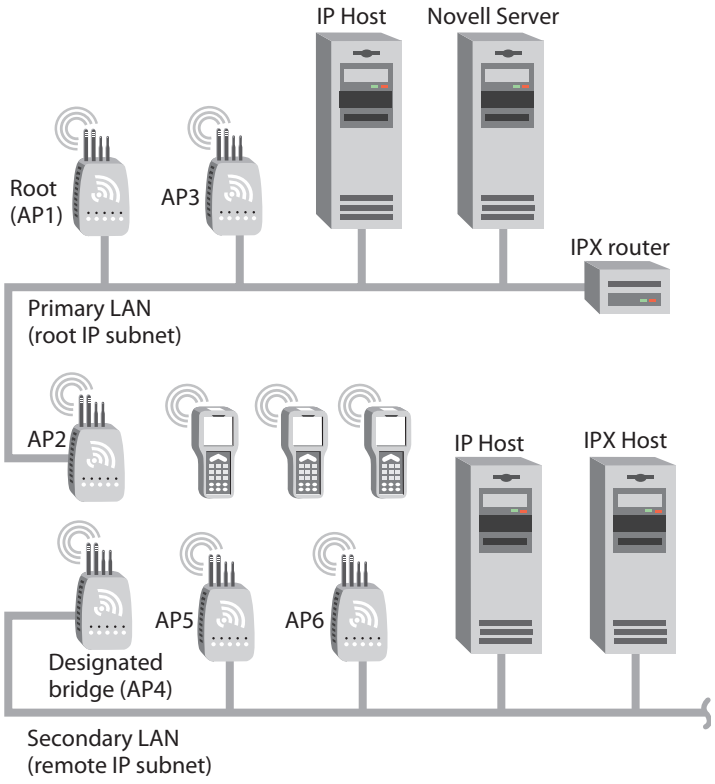
Subtype	Value
DIX-IPX-Socket	Socket value in hexadecimal.
DIX-EtherType	Specify the registered DIX type in hexadecimal.
SNAP-IP-TCP-Port	Port value in hexadecimal.
SNAP-IP-UDP-Port	Port value in hexadecimal.
SNAP-IP-Protocol	Port value in hexadecimal.
SNAP-IPX-Socket	Socket value in hexadecimal.
SNAP-EtherType	SNAP type in hexadecimal. To filter on both SNAP type and OUI, use advanced filters.
802.3-IPX-Socket	Socket value in hexadecimal.
802.2-IPX-Socket	Socket value in hexadecimal.
802.2-SAP	802.2 SAP in hexadecimal.

Filter Examples

These examples illustrate how to set both Ethernet and IP tunnel filters to optimize network performance. The next illustration includes:

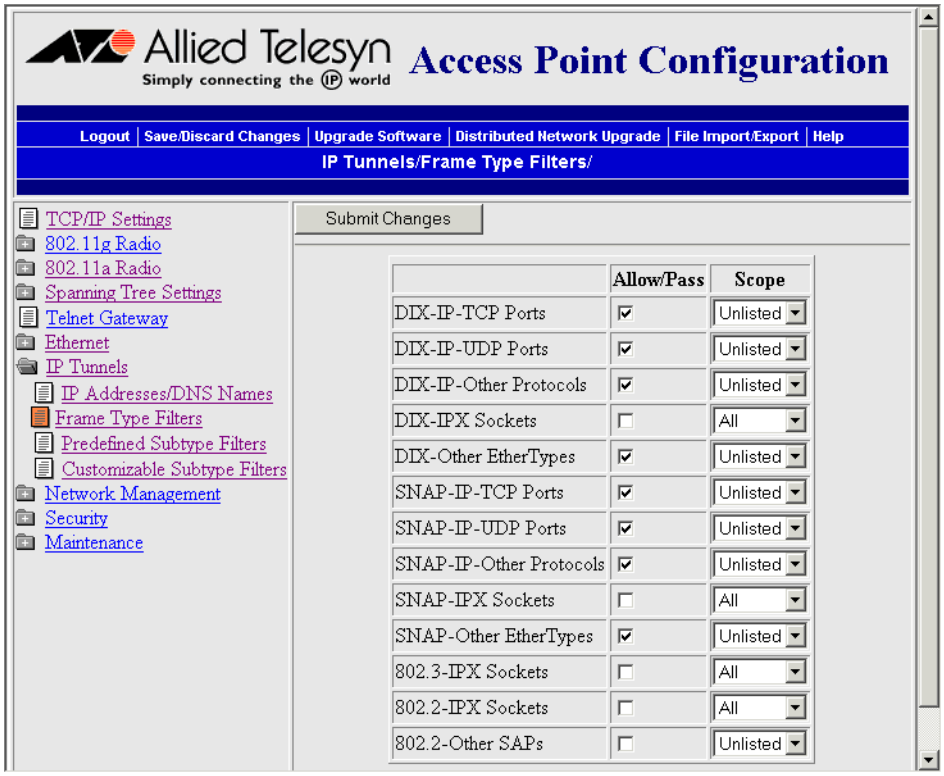
- wireless end devices using TCP/IP to communicate with other devices.
- a secondary LAN containing IP and IPX hosts, linked by AP2 and AP4.
- an IPX router connecting to another Novell network.
- DIX and 802.3 SNAP frames.

This illustration shows a typical network that will be used in the next examples.



Example 1 The root (AP1), AP3, AP5, and AP6 service only wireless end devices. These access points need to pass IP traffic, but not pass IPX traffic that does not need to be forwarded to the primary or secondary LAN.

For this example, set these options on the Ethernet Frame Type Filters screen. No subtype filters are needed.

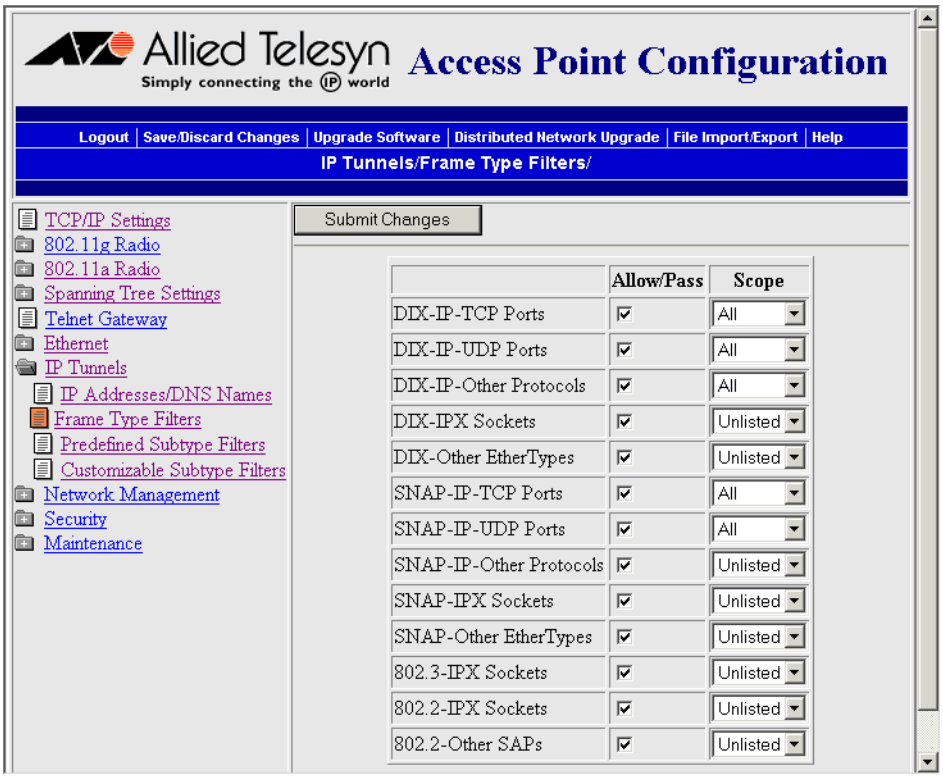


Example 2 AP2 and AP4 (designated bridge) service end devices and the IP host and IPX host on the secondary LAN. Also, these access points pass IPX traffic.

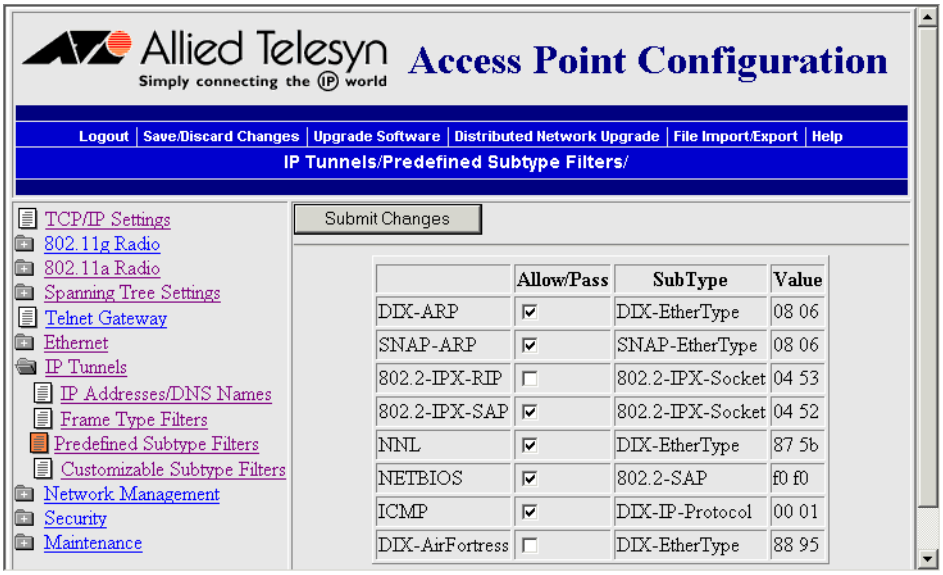
The IPX router in this network periodically sends IPX RIP frames for coordinating with other routers. These do not need to be forwarded to the secondary LAN, because the secondary LAN does not contain a router.

To filter the IPX RIP frames, you need to configure subtype filters. This example sets filters for three different cases: DIX, 802.2, and 802.3 SNAP frames. In many actual networks, only one type of filter is required, because all stations are configured using one of the three options.

For this example, set these options on the Ethernet Frame Type Filters screen.



In the Predefined Subtype Filters screen, set the 802.2-IPX-RIP field to drop 802.2, DIX, and 802.3 frames.



Example 3 If you have a DHCP server on a Windows NT server and you want to use this DHCP server to assign TCP/IP parameters to end devices on a remote IP subnet, you need to set these filters to allow for the necessary IP tunneling.

1. On the root access point, set these filters:
   - ❒ On the IP Tunnels screen, check the Allow IP Multicast check box.
   - ❒ In the IP Tunnel Frame Type Filter table, configure DIX-IP-UDP Ports to pass all frames.
2. On the access point at the endpoint of the IP tunnel, set this filter:
   - ❒ In the IP Tunnel Frame Type Filter table, configure DIX-IP-UDP Ports to pass all frames.

Example 4 If you have a Linux or Unix DHCP server and want to use this DHCP server to assign TCP/IP parameters to end devices on a remote subnet, you need to set this filter to allow for the necessary IP tunneling:

- ❒ In the IP Tunnel Frame Type Filter table, configure DIX-IP-UDP Port to pass all frames.

Comparing IP Tunnels to Mobile IP

The AT-WA7500 and AT-WA7501 access points support IP tunneling, which allows end devices to roam across different subnets (routers) without having to change IP addresses. IP tunneling supports IETF RFC 1701 using GRE and the same encapsulation technique as mobile IP. IP tunnels technology is designed primarily to operate in local environments, where handheld or vehicle-mounted devices may move rapidly between access point coverage areas on a subnet (although it is possible to attach a geographically remote subnet through an IP tunnel).

The Internet Engineering Task Force developed RFC 2002, IP Mobility Support, commonly referred to as mobile IP, to provide mobility for IP hosts. Mobile IP is designed primarily to address the needs of wireless end devices that may move between geographically separated locations.

The two technologies are complimentary and may coexist. Both protocols use similar encapsulation to forward frames to or from end devices that have roamed away from a root IP subnet. The root access point functions much like a mobile IP home agent; an access point attached to the remote end of an IP tunnel functions much like a mobile IP foreign agent.

Table 46. IP Tunnels and Mobile IP Comparison

Issue	IP Tunneling	Mobile IP
Software compatibility	No changes are required to existing IP software stacks in end devices.	Requires a mobile IP client software stack in end devices.
Addressing limitations for IP end devices	Requires that end device IP addresses belong to the root IP subnet.	None.
Security	Guest addresses are not used. Data link security.	Mobile IP authentication is required for “guest” access to foreign subnets.
Roaming detection	Data link indications facilitate fast roaming with no added broadcast traffic.	Foreign agent advertisements.
Roaming restrictions	Currently, roaming is limited to a single network that may include multiple IP subnets.	None.
Roaming support for non-IP protocols	Configurable using IP filters.	None.
Scalability	No practical limitations using IGMP.	Has no inherent limitations.

Table 46. IP Tunnels and Mobile IP Comparison (Continued)

Issue	IP Tunneling	Mobile IP
Special network software	Standard network feature. No additional network software is required.	Requires home and foreign agents located on each network or subnetwork.

Configuring Global Parameters

Global parameters are configured on the root access point and on any other access point that is a root candidate (does not have a root priority of 0). The root access point sends these settings to all other access points in the spanning tree. You should set the same global parameters for the root access point and its backup candidates. Any global parameters you set on the root access point will override those you set in other access points.

Configuring Global Flooding

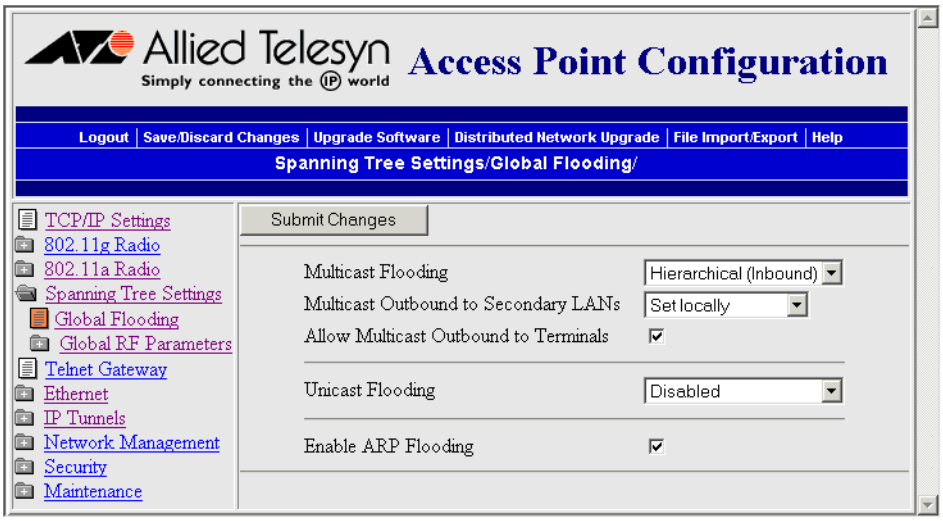
When the destination address is unknown, most bridges flood frames on all ports. Most wireless end devices operate at lower speeds than the Ethernet can support; therefore, indiscriminate flooding from a busy Ethernet network can consume a substantial portion of the available wireless bandwidth and reduce system performance. On the access point, you can set flooding control options for both unicast and multicast frames to free up bandwidth and improve system performance.

Access points try to forward frames to the port with the shortest path to the destination address. When the access point has not learned the direction of the shortest path, you can configure it to flood the frames in certain directions to try to locate the destination address.

ARP requests are multicast frames that are periodically sent out to all devices on the Ethernet network. An ARP cache is a table of known MAC addresses and their IP addresses that the access point maintains. When an access point receives an ARP request, it checks its ARP cache to determine if the destination end device's IP address is known.

To configure global flooding

1. From the main menu, click Spanning Tree Settings > Global Flooding. The Global Flooding screen appears.



2. Configure the Global Flooding parameters. For help, see the next table.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Table 47. Global Flooding Parameter Descriptions

Parameter	Explanation
Multicast Flooding	Determines the flooding structure when this access point receives inbound multicast frames on non-root ports with unknown destination addresses: Disabled: You do not want the access point to flood any inbound multicast frames. Universal: The access point forwards the multicast frame to every port. This option uses more bandwidth. Use this option if the root access point is supporting more than one wireless hop to ensure that ARP requests and multicast traffic are distributed. Hierarchical: The access point forwards the multicast frame only to the port to which the root access point is attached.
Multicast Outbound to Secondary LANs	Appears only if Multicast Flooding is enabled. Specifies if outbound multicast frames with unknown destination addresses are flooded toward secondary LANs: Enabled: The root access point controls flooding for all the designated bridges on secondary LANs. Enabling this parameter makes managing secondary LANs easier because you do not need to set secondary LAN flooding parameters. Set Locally: The designated bridges control flooding on their LANs.

Table 47. Global Flooding Parameter Descriptions (Continued)

Parameter	Explanation
Allow Multicast Outbound to Terminals	Appears only if Multicast Flooding is enabled. Determines if outbound multicast frames with unknown destination addresses are flooded toward end devices. Typically, this parameter is checked. However, if your wired devices do not need to initiate communication with wireless end devices, you may want to clear this check box.
Unicast Flooding	Determines the flooding structure when this access point receives inbound unicast frames on non-root ports with unknown destination addresses: Disabled: You do not want the access point to flood any inbound unicast frames. Universal: The access point forwards the unicast frame to every port. This option uses more bandwidth. Hierarchical: The access point forwards the unicast frame only to the port to which the root access point is attached.
Unicast Outbound to Secondary LANs	Appears only if Unicast Flooding is enabled. Specifies if outbound unicast frames with unknown destination addresses are flooded toward secondary LANs: Enabled: The root access point controls flooding for all the designated bridges on secondary LANs. Enabling this parameter makes managing secondary LANs easier because you do not need to set secondary LAN flooding parameters. Set Locally: The designated bridges control flooding on their LANs.
Allow Unicast Outbound to Terminals	Appears only if Unicast Flooding is enabled. Determines if outbound unicast frames with unknown destination addresses are flooded toward end devices.

Table 47. Global Flooding Parameter Descriptions (Continued)

Parameter	Explanation
Enable ARP Flooding	Check this check box to enable ARP flooding. When an access point receives an ARP request, it checks its ARP cache to determine if the destination end device's IP address is known. If you enable ARP flooding and: ❒ the destination end device is known, the access point translates the ARP request into a unicast frame, which is only forwarded to the destination end device. Therefore, all end devices do not need to wake up to listen to the ARP request, which saves battery life. ❒ the destination end device is not known, the access point forwards the ARP request based on its flooding and filtering settings. If you disable ARP flooding, the access point ignores ARP requests for destination end devices that are not in its ARP cache. You should only use this option if you have no IP devices in your wireless network.

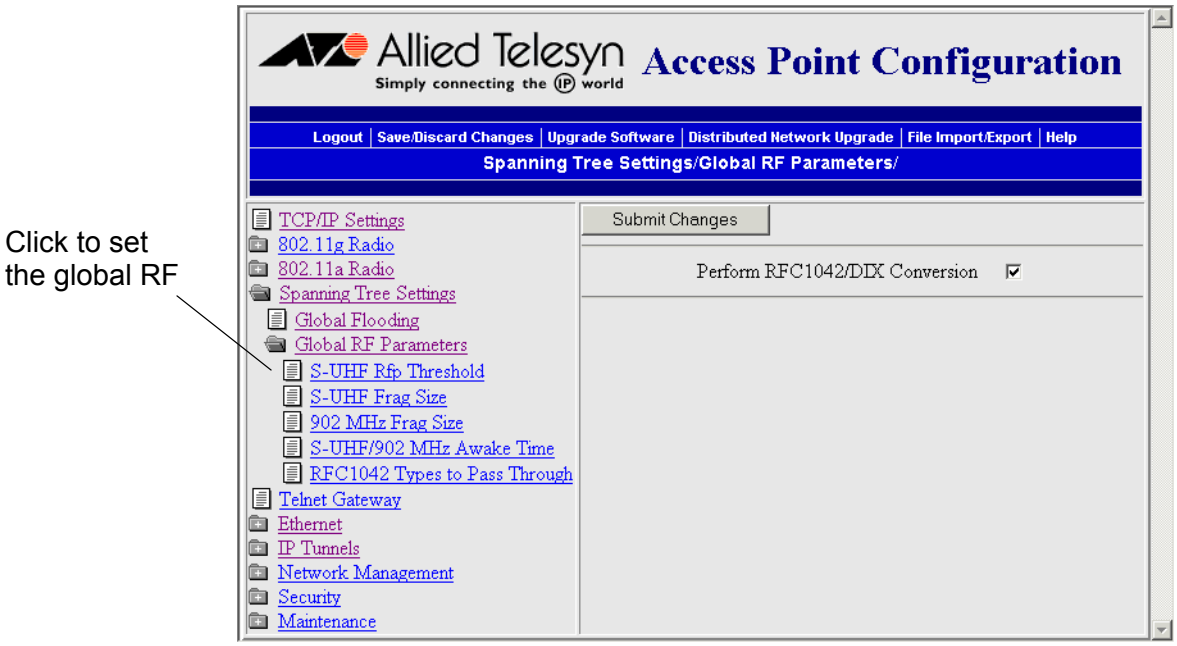
Configuring Global RF Parameters

Use global RF parameters to set various parameters on the access points. If you are configuring the root access point and you check the Set Globally check box, the value for that parameter is set globally for all access points and wireless end devices in the network. If you are configuring the root access point and you clear the Set Globally check box or if you are not configuring the root access point, each device uses its local setting.

To configure global RF parameters

1. From the menu, click Spanning Tree Settings > Global RF Parameters.

The Global RF Parameters screen appears.



2. Configure the global RF parameters. Click the links in the Global RF Parameters menu to set more parameters. For help, see the next table.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Table 48. Global RF Parameter Descriptions

Parameter	Explanation
Perform RFC1042/ DIX Conversion	Determines how the access point will handle the conversion of RFC1042/DIX frames that are received on its radio ports. Check this check box if the frames that are received and have a protocol type equal to a value in the "RFC1042 types to pass through" list are forwarded without conversion. If the frame has a protocol type that is not found in the list, it will be converted to DIX format before it is forwarded. Clear this check box if the frames that are received are forwarded without conversion; that is, when a SNAP frame is received from a radio with an OUI (Organizationally Unique Identifier) equal to 000000, it will be forwarded without conversion.
S-UHF Rfp Threshold (S-UHF radios only)	Specifies the largest data frame that can be transmitted without reserving airtime. Air time is normally reserved to help prevent collisions with other transmitters; however, when the amount of data is small enough, sending the data may be more effective than creating the reservation.
S-UHF Frag Size (S-UHF radios only)	Specifies the largest data frame that can be transmitted without fragmentation. On certain radios, fragmentation does not occur unless the radio detects interference. Larger frame sizes can improve throughput on a reliable connection, while smaller frame sizes can improve throughput on a poor connection.
902 MHz Frag Size (902 MHz radios only)	Specifies the largest data frame that can be transmitted without fragmentation. On certain radios, fragmentation does not occur unless the radio detects interference. Larger frame sizes can improve throughput on a reliable connection, while smaller frame sizes can improve throughput on a poor connection.

Table 48. Global RF Parameter Descriptions (Continued)

Parameter	Explanation
S-UHF/902 MHz Awake Time (S-UHF and 902 MHz radios only)	Specifies the amount of time that a wireless end device stays awake when radios are inactive. A sleeping device is less responsive to radio activity; however, the longer a device is kept fully awake, the larger the drain on the battery. You should set a device to stay awake long enough to receive an expected reply to a transmission and short enough to reduce power consumption. The awake time can be set to a number from 0 to 250 tenths of a second.
RFC1042 Types to Pass Through (802.11g, 802.11b, or 802.11a radios only)	If the RFC1042/DIX Conversion field is Enabled, this parameter specifies values for protocol types that are to be passed without conversion. The list includes the Apple Talk protocol type, value 80F3. Values entered in this parameter represent the protocol types of frames that will be passed without conversion to DIX format.

Chapter 6

Configuring Security

This chapter explains how to use different security solutions to ensure that you have a secure wireless network. This chapter covers these topics:

Understanding Security

The AT-WA7500 and AT-WA7501 access points provide many different security features and solutions that you can use to create a secure wireless network. To create a secure wireless network, you need to be concerned about:

- securing your backbone. Only authorized users should be able to communicate with your network.
- keeping your data private. Make it difficult for an eavesdropper, such as a rogue access point, to monitor your data.
- authenticating wireless end devices. End devices must prove who they are before they are allowed to communicate with your network.

Depending on the radios in the access point and the amount of security you need in your network, you can implement one or more of the security solutions in the following table.

Table 49. AT-WA7500 and AT-WA7501 Security Solutions

Security Type	Secure Backbone	Data Privacy	Client Authentication
Change default parameters	X		
Disable access methods	X		
Enable secure IAPP	X		
Enable secure wireless hops	X		X
Use a password server to manage access point logins	X		
Configure a VLAN for each radio	X		
Use an Access Control List (ACL)			X
Use WEP 64/128/152 security		X	
Use an 802.1x security solution	X	X	X
Use Wi-Fi Protected Access (WPA)	X	X	X

These security features and solutions are listed below in the order of amount of security and ease of use (most basic/least secure to most secure). Allied Telesyn recommends you configure your wireless network for the maximum possible security that you deem necessary for the integrity of your network.

1. Change the SSID from its default value of ATILAN and check the Disallow Network Name of 'ANY' check box. For help, see Chapter 4, "Configuring the Radios" on page 96.

2. Enable/disable access methods. For example, if you are not using telnet sessions to configure or manage your access point, you can disable this access method. For help, see "Controlling Access to Access Point Menus" on page 174.

3. Use a password server to maintain a list of authorized users who can configure and manage the access points. You can either use an external RADIUS server or you can use any access point's embedded authentication server (EAS).

   Or change the default login for users who need to configure or manage the access point. For help, see "Setting Up Logins" on page 176.

4. Create a secure spanning tree, which between access points, and includes secure IAPP and secure wireless hops. For help, see "Creating a Secure Spanning Tree" on page 181.

5. Use a RADIUS server to maintain an access control list (ACL), which is a list of MAC addresses of end devices that can connect to the network through access point. You can either use an external RADIUS server or you can use any access point's embedded authentication server (EAS). For help, see "Using an Access Control List (ACL)" on page 184.

6. Configure VLANs that separate secure and non-secure communications in your network. For help, see "Configuring VLANs" on page 187.

7. Implement one of these mutually-exclusive security solutions (on each service set) to ensure secure communications between the access points and wireless end devices in your network:

   Use basic WEP 64/128/152 security. You can configure up to four different WEP keys on the access point and most wireless end devices, and then you specify which key is being used to encrypt data. You should periodically change which WEP key these devices use. 802.11g and 802.11b radios support WEP 64/128 security, and 802.11a radios support 64/128/152 security. For help, see "Configuring WEP 64/128/152 Security" on page 189.

Use an 802.1x security solution. 802.1x security provides a framework to authenticate user traffic to a protected wireless network. Using 802.1x security provides secure data transmission by creating a secure spanning tree and dynamically rotating the WEP keys. You configure the access point as an authenticator. For the authentication server, you can either use an external RADIUS server or you can use the access point's embedded authentication server (EAS). For help, see "Implementing an 802.1x Security Solution" on page 192.

Use Wi-Fi Protected Access (WPA) security. WPA is a strongly enhanced, interoperable Wi-Fi security that addresses many of the vulnerabilities of Wired Equivalent Privacy (WEP). For help, see "Configuring Wi-Fi Protected Access (WPA) Security" on page 199.

For help troubleshooting security, see "Troubleshooting Security" on page 255.

When You Configure Different SSIDs with Different Security Settings

You can configure each 802.11g and 802.11a radio with up to four SSIDs or service sets. Although each service set shares one physical radio configuration, you can configure each service set with a different security configuration. Also, you can configure each service set for a separate VLAN. For example, you can configure:

- primary service set for WPA/PSK.
- secondary 1 service set for WPA/802.1x and VLAN 13.
- secondary 2 service set for static WEP and an ACL.
- secondary 3 service set for Dynamic WEP/802.1x and VLAN 150.

Note that using multiple services sets is not part of the Wi-Fi standard. When multiple service sets are enabled, the SSID is hidden in the beacons, which is similar to checking the Disallow Network Name of 'ANY' check box. The access point master radio only sends a beacon from the primary service set. However, if an end device's radio sends a probe request for an SSID that belongs to a secondary service set, then the access point radio will send a probe response from that service set.

Many end device radios do not support using multiple service sets to implement a mixed security environment. The radios do not understand different security information coming from the beacons and probe responses. This means:

- if any type of security is set on the primary service set, then the secondary service sets should also the same type of security.
- if no security is set on the primary service set, then the secondary service sets cannot use any type of security.

For example, you have an access point with an 802.11g radio. You configure the primary service set for WPA/PSK and you do not configure any security for the secondary 1 service set. An older end device with an

802.11b radio is configured with no security and you expect it to associate with the secondary 1 service set. However, when the end device receives the beacon from the access point that indicates that some type of security is being used, the end device does not communicate with the access point.

Another important consideration is that the service set that allows wireless hops should have the strongest security configuration possible for your environment. Do not enable wireless hops on the ports that have no security. WAPs configured on the other service sets will hear the unencrypted hellos on the wireless hop port and those WAPs will attach to the spanning tree, even though they should not.

When You Include Multiple RADIUS Servers on the RADIUS Server List

You can use multiple RADIUS servers to act as password servers, to support ACLs, to use in an 802.1x security solution as authentication servers, and to use in an WPA/802.1x security solution as authentication servers. If you don't configure the server port map, the access point uses the first RADIUS server (Server 1) in the list as the main server. Other servers are simply backup servers.

- If the first RADIUS server responds and the client's information does not appear in that server's database, the client is blocked. The access point does not check the databases on any other RADIUS servers.
- If the first RADIUS server goes down during the operation and a RADIUS server lookup needs to occur, the authenticator access point will time out looking for the first server. Then, the access point looks for the next server in the list. If the authenticator access point finds the next server, it stays with that server forever, even if the first server comes back. If the backup server goes down, the authenticator access point continues looking down the list and eventually wraps around to the first server again.

However, you can configure the server port map so that the access point uses different RADIUS servers to serve different ports.

To configure the server port map

- From the main menu, click Security > RADIUS Server List > Server Port Map. The Server Port Map screen appears with the IP Address/ DNS Name column populated with the RADIUS servers that you configured in the Server Selection screen.

For example, you can select one RADIUS server to service parent access points authenticating child access points using IAPP authentication by checking the check box in the IAPP Authentication column. Then, you can select another RADIUS server to service access points authenticating end devices by checking the check box for the appropriate service set.

Controlling Access to Access Point Menus

There are several ways that you can manage who can configure and manage the access points in your network:

- Enable/disable access methods.
- Set up individual logins.
- Change the default logins and create a read-only login.

The next sections explain how to implement these strategies.

Enabling Access Methods

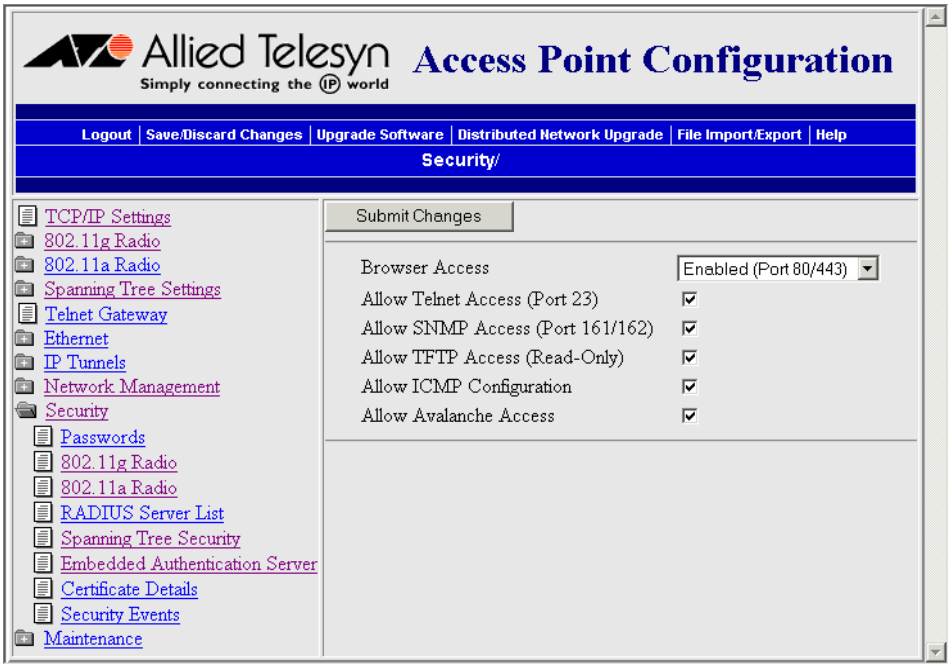
There are five access methods that you can enable or disable depending on how you want users to be able to configure or manage the access points:

- Web browser interface (HTTP or HTTPS)
- Telnet session
- Any SNMP management station
- TFTP
- Programs that uses ICMP echo
- Wavelink Avalanche client management system

All access methods are enabled by default. You may want to disable any of these methods that you will not use to prevent access by an unauthorized method.

To enable or disable access methods

1. From the main menu, click Security. The Security screen appears.



2. Enable or disable the access methods that users can use to connect to the access point. For help, see the next table.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Table 50. Security Parameter Descriptions

Parameter	Description
Browser Access	Determines if users can use a web browser to configure or manage this access point. Browser access is through either port 80 or port 443. Choose Secure-Only if you want to force users to log in using the secure web browser (HTTPS) interface. Secure-only access is through port 443.

Table 50. Security Parameter Descriptions (Continued)

Parameter	Description
Allow Telnet Access (Port 23)	Determines if users can use a telnet session (or communications program) to configure or manage this access point. Do not clear this check box if you plan to configure the Telnet Gateway and allow wireless clients to upgrade the access point over the telnet port. For details, see page 210.
Allow SNMP Access (Port 161/ 162)	Determines if users can use MobileLAN manager or another SNMP management station to configure or manage this access point.
Allow TFTP Access (Read-Only)	Determines if users can use TFTP clients to exchange files with the access point.
Allow ICMP Configuration	Determines if users can use another program that uses ICMP echo (PING) to set the IP address or restore factory defaults on this access point.
Allow Avalanche Access	Determines if users can use the Wavelink Avalanche client management system to manage this access point.

Setting Up Logins

To ensure login security for configuring or maintaining the access points, you should either use a password server (typically an EAS or another RADIUS server) or change the default user name and password.

To use the password server, you must have:

- a password server on the network that contains the user name/ password database. For help, see “Configuring the Access Point to Use a Password Server” on page 177. You can either configure an EAS or you can use an external RADIUS server as a password server.
- access points, which are the RADIUS clients.

If you use a password server, you enable RADIUS for login authorization. That is, when a user attempts to log in to the access point, the user must enter a user name and password. This login is sent through the RADIUS client (access point) to the RADIUS server. The server compares the login to its list of authorized logins. If a match is found, the server returns an access-accept frame and the user is logged in to the access point with read/write privileges.

If no RADIUS server is available when the user attempts a login and the Allow Service Password check box is checked, the service password is checked. If the login does not match the service password, the login fails.

Note
Each time the service password login attempt fails, the process may take up to 8 seconds.

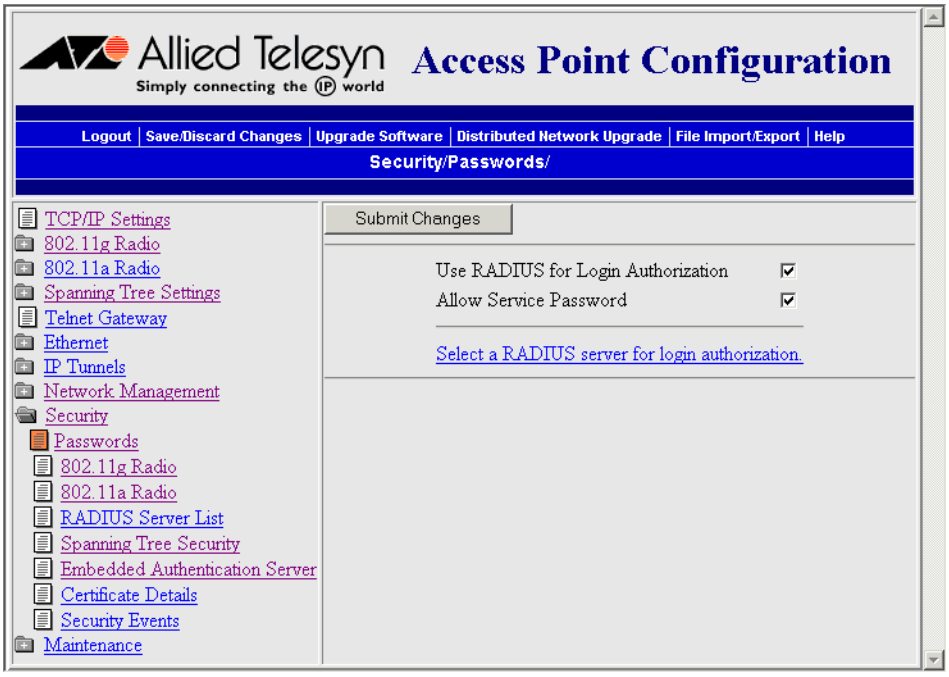
If you do not want to enable RADIUS authorization, you should change the default login user name and password. You may also want to change the read-only password. For help, see "Changing the Default Login" on page 178.

Configuring the Access Point to Use a Password Server

If you use a password server to manage users who can log in to this access point, you need to tell this access point how to communicate with the password server and then you need to configure the password server. The password server can either be an EAS or an external RADIUS server.

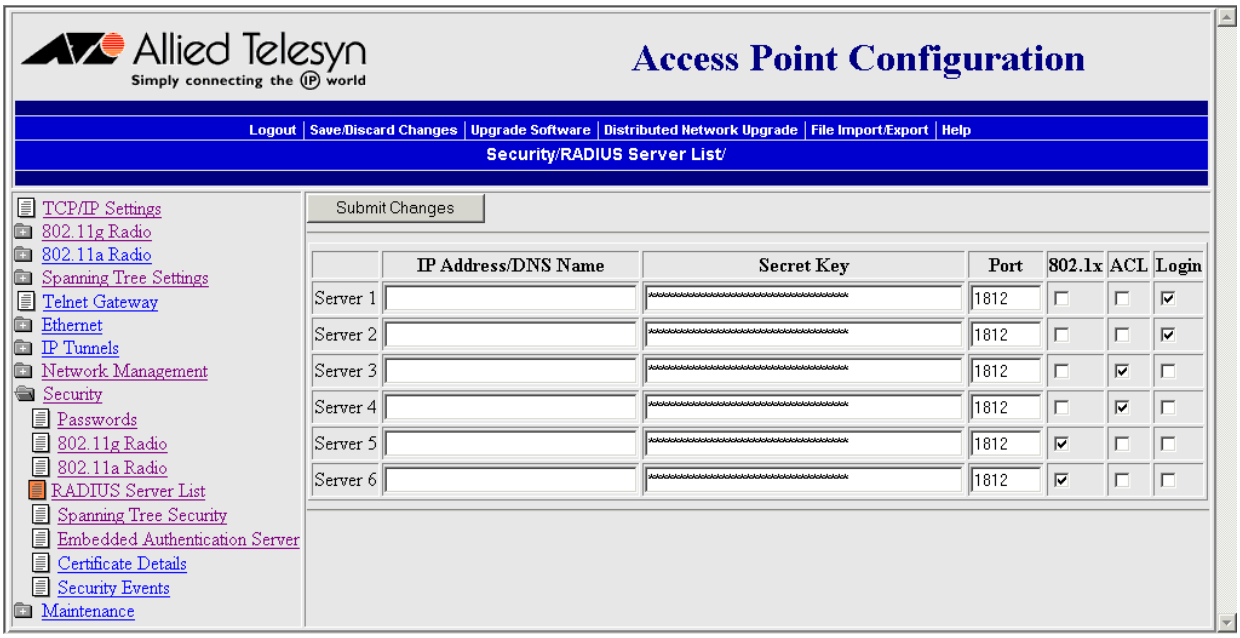
To configure the access point to use a password server

1. From the main menu, click Security > Passwords. The Passwords screen appears.



2. Check the Use RADIUS for Login Authorization check box.
3. (Optional) Make sure the Allow Service Password check box is checked.
4. Click Submit Changes to save your changes.

5. Configure the password server by clicking Select a RADIUS server for login authorization. The RADIUS Server List screen appears.



6. For each password server, enter the IP address or DNS name, enter the shared secret key, port number, and check the Login check box.

> **Note**
> If you enter more than one password server, see page 130 for a description of how the access point uses the servers.

7. Configure the password server database:

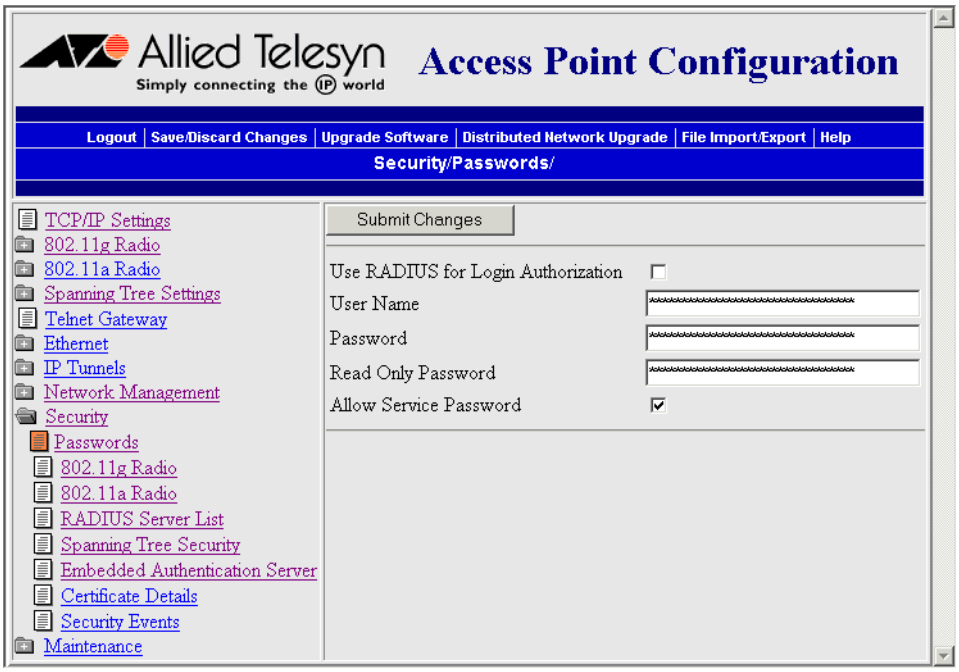
   - In the EAS database, in the Type field choose Login and then enter the user name and password for each login. For help, see Chapter 7, “Configuring the Embedded Authentication Server (EAS)” on page 204.
   - For help configuring an external RADIUS server database, see the documentation that came with your server.

Changing the Default Login

If you are not using a password server to authorize user logins, you should change the default user name and password and create a read-only password.

To set up logins

1. From the main menu, click Security > Passwords. The Passwords screen appears.



2. Verify that the Use RADIUS for Login Authorization check box is cleared.

3. Click Submit Changes to save your changes.

4. Configure the parameters. For help, see the next table.

5. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Once the changes are activated, you must enter these new values when you use a web browser or telnet to connect to this access point.

Table 51. Password Parameter Descriptions

Parameter	Description
Use RADIUS for Login Authorization	Determines if you are using a password server to authenticate end devices that can communicate with this access point. Clear this check box.
User Name	Enter the user name you need to use to log in to this access point. This parameter can be from 0 to 16 characters long. If you leave the user name and password fields blank, a user will not need to log in to the access point.
Password	Enter the password you need to use to log in to this access point. This password gives you read and write access to the access point configuration. This parameter can be from 0 to 16 characters long. If you leave the user name and password fields blank, a user will not need to log in to the access point.
Read Only Password	Enter the password you need to use to log in to this access point. This password gives the user read-only access to the access point. This user is able to view the configuration and execute diagnostics but cannot perform any tasks that affect the operation of the access point, such as changing configuration options, rebooting, or downloading software. To disable this password, delete it.
Allow Service Password	If the user enters a login that does not match either the user name and password or the read only password, check this check box to allow the login to be checked against the service password. Allied Telesyn Technical Support may use this service password if they need to troubleshoot this access point.

Creating a Secure Spanning Tree

When you configure a radio to use 802.1x security, you automatically enable spanning tree security, which can be used for both wired and wireless access points (WAPs). However, if you configure a radio to use another security solution, you may want to still create a secure spanning tree. A secure spanning tree has two functions:

1. To require authentication of any access point attempting to join the spanning tree.

2. To provide encryption of critical Inter-Access Point Protocol (IAPP) frames.

There are three authentication methods that you can use to secure the spanning tree: Simple Wireless Authentication Protocol (SWAP), TTLS, or TLS.

SWAP is an proprietary protocol that is based on the EAP-MD5 challenge. Since it requires less processing power, it requires less memory and you can use it on all access points. Also, SWAP does not require an authentication server so it is easier to configure. With these advantages, SWAP is sufficient for most users. TTLS and TLS are industry standard protocols. However, they require more administrative support.

When deciding on which type of spanning tree security to use, the supplicant access point and the authenticator will negotiate an authentication method that can be used by both. If the Allow SWAP check box is checked on both access points, SWAP will always be used. If the Allow SWAP check box is cleared on one or both of the access points, either TTLS or TLS will be used, depending on the setting of the Preferred Protocol field of the supplicant access point.

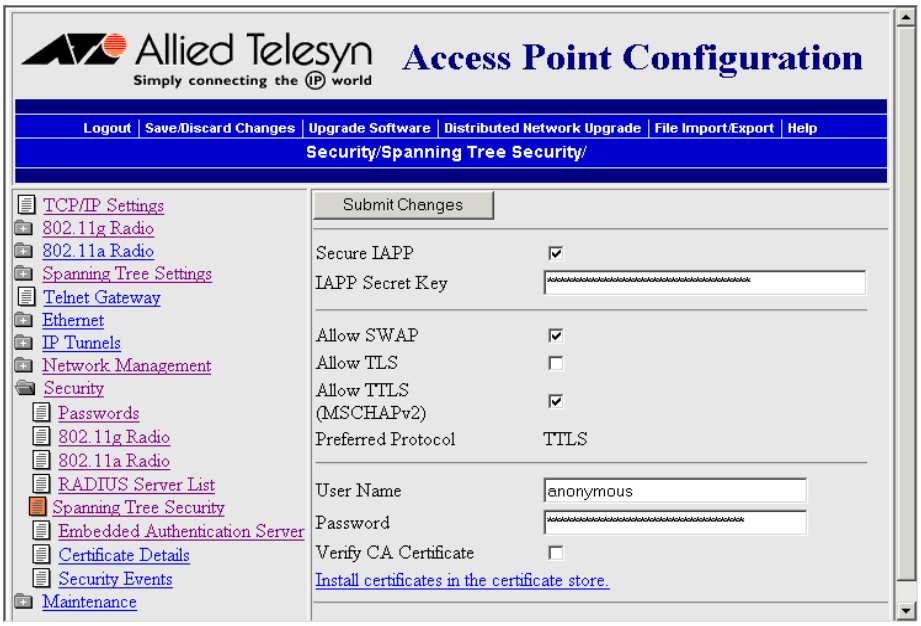
Note these potential problems:

- If you enable secure IAPP on a root access point that is running software release 1.80 or later and other access points in your network are running an earlier software release than 1.80, the access points with the earlier software release will not attach to the root. The access points with the earlier software release do not support secure IAPP. If you want to use secure IAPP, upgrade all access points to software release 1.80.
- If you enable secure IAPP on a non-root access point and the root access point has secure IAPP disabled, the access points will form separate spanning trees with the same LAN ID. If you want to use secure IAPP, enable secure IAPP on all access points.

To create a secure spanning tree

Note
You do not need to perform this procedure if you are implementing an 802.1x security solution. 802.1x authentication automatically enables secure IAPP and secure wireless hops. See “Implementing an 802.1x Security Solution” on page 192.

1. From the main menu, click Security > Spanning Tree Security. The Spanning Tree Security screen appears.



2. Check the Secure IAPP check box.
3. Click Submit Changes to save your changes.
4. In the IAPP Secret Key field, enter a secret key. This secret key must be between 16 and 32 bytes.
5. Determine how the access points authenticate to the network:
   - ❒ Check the Allow SWAP check box if you have older access points or you are not implementing an 802.1x security solution.
   - ❒ Check the Allow TLS check box, if you are implementing an 802.1x security solution and you want to use TLS. The access point must have a server certificate loaded on it.
   - ❒ Check the Allow TTLS (MSCHAPv2) check box, if you are implementing an 802.1x security solution and you want to use TTLS. You must also enter a User Name and Password that matches an entry in the authentication server.

6. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

7. Repeat Steps 1 through 6 for each access point in your spanning tree. All access points must have the same IAPP secret key to communicate with each other.

In the access point that contains the master radio, click Maintenance > AP Connections. The AP Connections screen lists the station radios (including ones in other access points) that are communicating with the master radio. For help, see "Viewing AP Connections" on page 228.

Enabling Secure Communications Between Access Points and End Devices

There are several ways that you can ensure secure communications between access points and wireless end devices in your network:

- Use an access control list (ACL).
- Configure virtual LANs (VLANs).
- Configure WEP 64/128/152 security.
- Implement an 802.1x security solution.
- Configure Wi-Fi Protected Access (WPA) security.

The next sections explain how to configure these methods.

Using an Access Control List (ACL)

You can use an access control list (ACL) that contains the MAC addresses that are authorized to communicate with the network through the access point. The end devices do not need any special client software. To use the ACL, you must have:

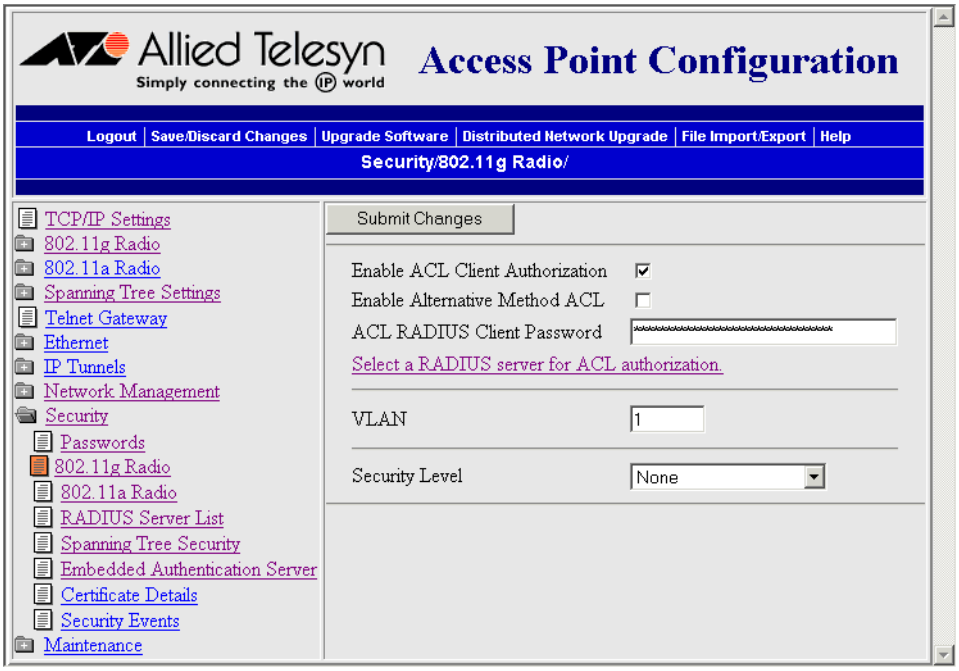
- a RADIUS server on the network that contains the ACL. You can either use an external RADIUS server or you can configure an EAS. For help, see Chapter 7, “Configuring the Embedded Authentication Server (EAS)” on page 204.
- access points, which are the RADIUS clients.

If the access point has two radios, or if the access point contains one 802.11g or 802.11a radio with multiple service sets, you can use an ACL for one radio and another type of security for the other radio.

For example, you have some end devices that have an 802.1x supplicant and you have some end devices that do not have a supplicant. You can enable one radio to use 802.1x security and the other radio to use an ACL. You can also use one ACL for both radios. However, you cannot use a different ACL for each radio.

To use an ACL

1. From the main menu, click Security and then click the radio service set you are configuring. The appropriate radio screen appears.



2. Check the Enable ACL Client Authorization check box if you want to use an ACL to authorize end devices to communicate with the network.

3. Click Submit Changes to save your changes.

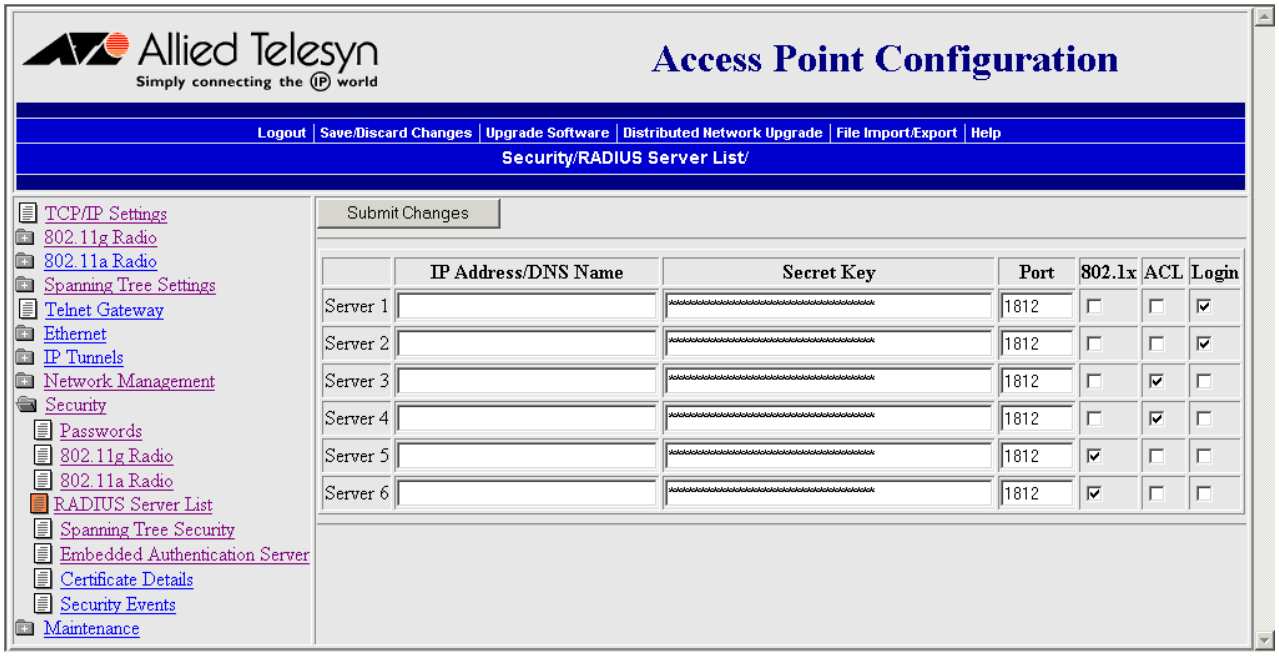
4. Normally, the access point issues RADIUS requests with the user name and password of the end device that is trying to communicate with the network.

   Check the Enable Alternative Method ACL check box if you want the access point to issue RADIUS requests with the user name and password both set to the MAC address of the end device that is trying to communicate with the network.

5. (External RADIUS server only) In the ACL RADIUS Client Password field, enter the password that is used to sign RADIUS access requests for all end devices attached to this access point. This password must match the password that is configured in the RADIUS server.

6. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

7. Configure the RADIUS server by clicking Select a RADIUS server for ACL authorization. The RADIUS Server List screen appears.



8. For each RADIUS server, enter the IP address or DNS name, enter the shared secret key, port number, and check the ACL or Login check box.

Note
If you enter more than one server, see page 130 for a description of how the access point uses the servers.

9. Configure the database. Enter the MAC address for each end device radio that is allowed to communicate with the network:

   - In the EAS database, in the Type field choose ACL and then enter the MAC address for each end device radio.

     Or, if you checked the Enable Alternative Method ACL check box, in the Type field choose Login and then enter the MAC address for each end device radio in both the user name and password fields.

     For help, see Chapter 7, “Configuring the Embedded Authentication Server (EAS)” on page 204.

   - For help configuring an external RADIUS server database, see the documentation that came with your server. In the database, you will also need to enter the ACL RADIUS client password. The default password is wireless (case-sensitive).

Configuring VLANs

Virtual LANs (VLANs) make it easy to create and manage logical groups of wireless end devices that communicate as if they were on the same LAN. You can group all wireless users on a particular VLAN in order to manage the IP address space differently. Or, you can use VLANs to separate secure and non-secure traffic. For example, you may grant your employees full access to your network, while routing all traffic from visitors to the Internet. The access points may be configured to participate in a properly configured VLAN.

You can configure each 802.11g and 802.11a radio with up to four SSIDs, creating up to four service sets. Each service set shares one physical radio configuration, but you may customize its security configuration. Therefore, each service set can be configured to support a separate VLAN.

However, an 802.11b radio can be configured with only one SSID. Therefore, each 802.11b radio can support only one VLAN, and you would need multiple 802.11b radios to implement multiple VLANs.

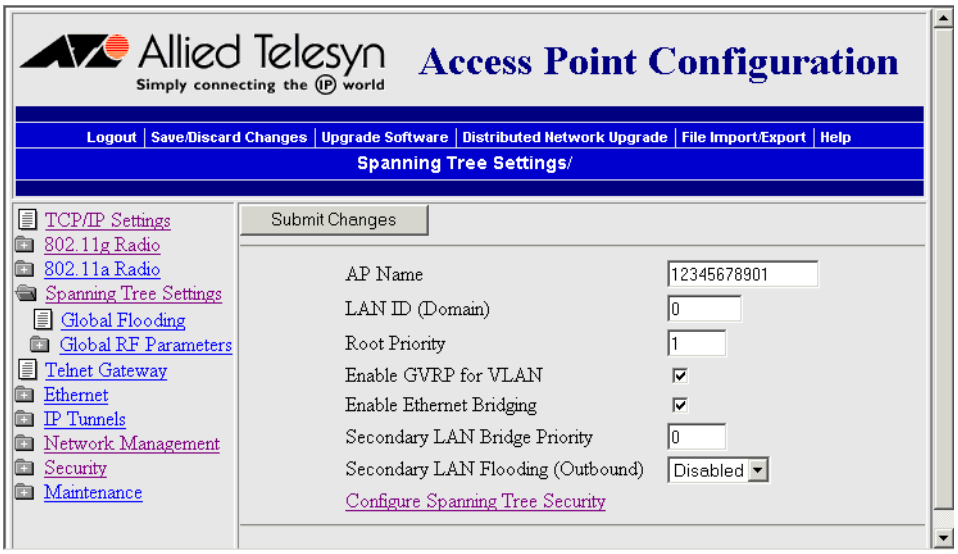
You configure each radio (or each service set) as a master radio with a unique SSID and security solution. Then, you distribute the SSID of the secure network to your end devices and the SSID of the non-secure network to your customers.

The access points support the 802.1Q standard for VLAN tagging. When the access point receives a frame from an end device, it applies the appropriate VLAN tag to the frame and then bridges the VLAN-tagged frame to the wired network. If you configure the VLAN field to 1, no VLAN tag will be applied and the frames will be put on the wired network as normal Ethernet frames. A VLAN-capable Ethernet switch receives the VLAN-tagged frame and routes it appropriately. Only VLAN-aware devices understand frames with VLAN tags; end devices only understand and accept frames that are meant for them that do not have a VLAN tag.

In order for the spanning tree to work, all access points must be on the same Native port on the Ethernet switch. The switch must be able to support a "hybrid" VLAN, which means the switch can support both VLAN-tagged and normal Ethernet frames on the switch port. The access point only encapsulates wireless traffic. Any communication with the access point across the wired network is always normal Ethernet traffic.

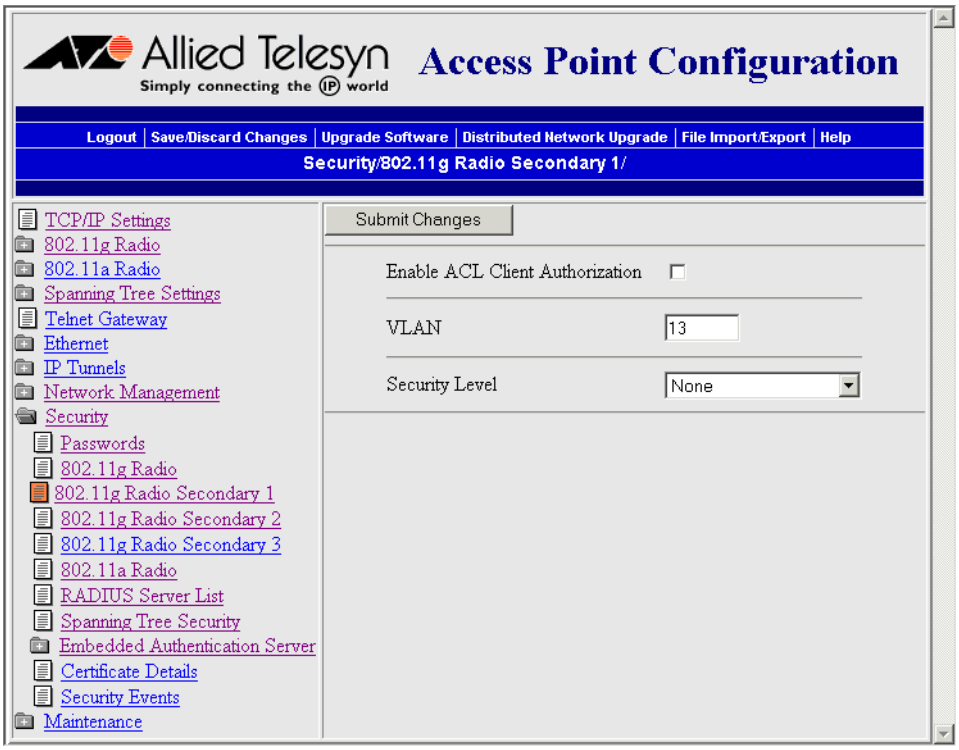
To configure a VLAN

1. From the main menu, click Spanning Tree Settings. The Spanning Tree Settings screen appears.



2. Check or clear the Enable GVRP for VLAN check box:.
   - ❒ Check the check box if the VLAN switch is configured to dynamically configure its ports based on the end devices' needs.
   - ❒ Clear the check box if the VLAN switch is statically configured to always forward specific VLANs to specific ports.
3. Click Submit Changes to save your changes.
4. From the main menu, click Security. If you have enabled more than the primary service set, you can configure each secondary service set for a different VLAN.

5. Under the Security link, click the radio service set you want to configure for the VLAN. This screen appears.



6. In the VLAN field, enter the VLAN number that encapsulates all frames received on this radio port. This value must match the values that are set in the VLAN-capable Ethernet switches on the primary LAN.

> **Note**
> The value in the VLAN field is also called the VLAN tag.

7. Repeat Steps 5 and 6 to assign a unique VLAN tag to each service set that you want to configure to support a VLAN.

8. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Configuring WEP 64/128/152 Security

You can configure static WEP keys to provide security between the access points and the wireless end devices. To use static WEP keys, your radios must support WEP encryption. All access points and wireless end devices on a particular network must use the same WEP encryption type and the same WEP transmit key. You should periodically change this WEP transmit key to prevent an unauthorized person with a sniffing tool from monitoring your network and discovering the WEP key.

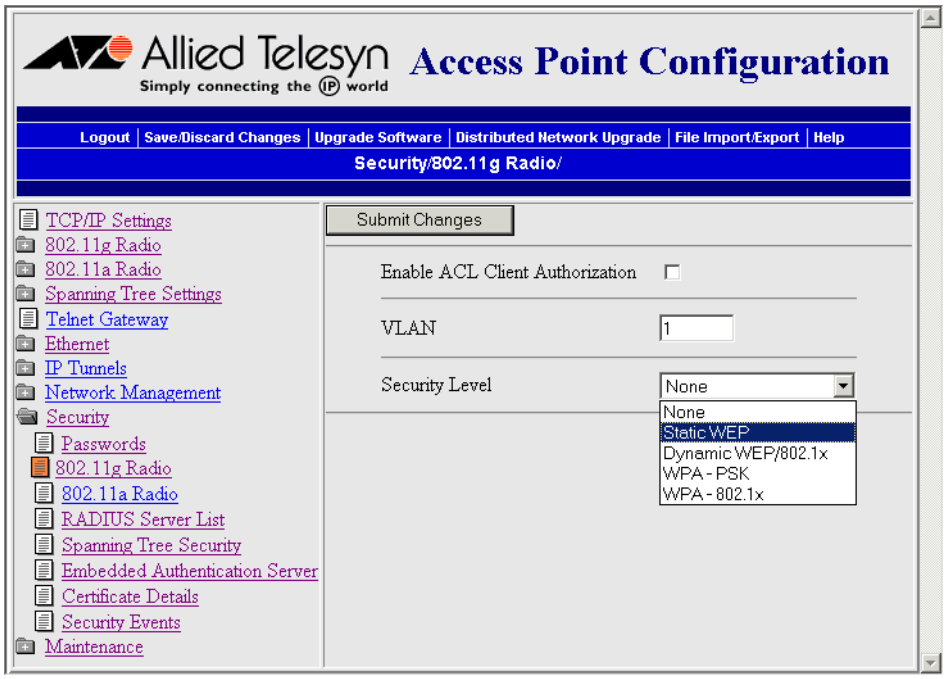
Since static WEP keys can be difficult to update, the AT-WA7500 and AT-WA7501 access products let you enter up to four WEP keys, and then pick a WEP transmit key (1-4). It is easier to rotate the WEP transmit key than to individually change all the WEP keys.

802.11g and 802.11b radios support WEP 64/128 security, and 802.11a radios supports 64/128/152 security:

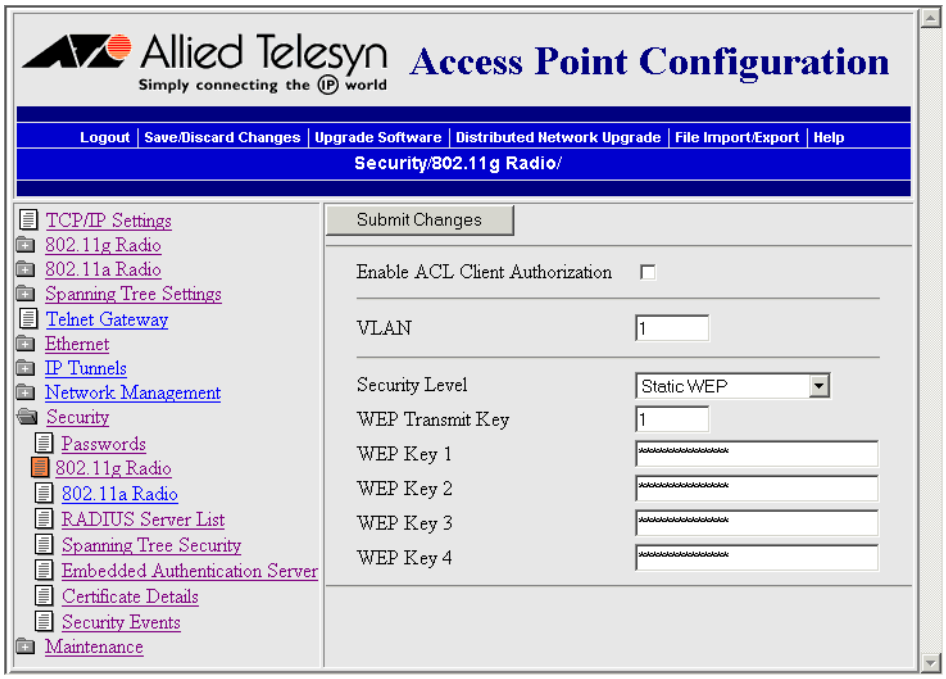
- WEP 64 has four 40-bit encryption keys and one 24-bit initialization vector (IV) key. Enter five ASCII characters or five hex pairs for the WEP keys.
- WEP 128 provides a higher degree of encryption protection. It has four 104-bit encryption keys and one 24-bit IV key. Enter 13 ASCII characters or hex pairs.
- WEP 152 provides the highest degree of encryption protection. It has four 128-bit encryption keys and one 24-bit IV key. Enter 16 ASCII characters or hex pairs.

To configure WEP 64/128/152 security

1. From the main menu, click Security and then click the radio service set you are configuring. The appropriate radio screen appears.
2. In the Security Level field, select Static WEP.



3. Click Submit Changes to save your changes. This screen appears.



4. Configure the parameters for WEP configuration. To ensure maximum security, configure each WEP key with a different WEP code. For help, see the next table.

5. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Table 52. WEP Security Parameter Descriptions

Parameter	Explanation
Security Level	Select Static WEP from the drop-down menu to use WEP 64/128/152 security.
WEP Transmit Key	Determines which of the four WEP keys this access point uses to transmit data.
WEP Key 1 WEP Key 2 WEP Key 3 WEP Key 4	For WEP 64, enter five ASCII characters or five hex pairs. For WEP 128, enter 13 ASCII characters or hex pairs. For WEP 152, enter 16 ASCII characters or hex pairs. To enter a hexadecimal key, prefix it with 0x. For example, the ASCII key ABCDE is equivalent to 0x4142434445.

Implementing an 802.1x Security Solution

You can implement 802.1x security in your network. The IEEE 802.1x standard provides an authentication protocol for 802.11 LANs. 802.1x provides strong authentication, access control, and key management, and lets wireless networks scale by allowing centralized authentication of wireless end devices.

The 802.1x authentication process uses a RADIUS server, which is the authentication server, and access points, which are the authenticators, to manage the wireless end device authentication and wireless connection attributes. Extensible Authentication protocol (EAP) authentication types provide devices with secure connections to the network. They protect credentials and data privacy. Examples of EAP authentication types include Transport Layer Security (EAP-TLS) and Tunneled Transport Layer Security (EAP-TTLS).

To implement 802.1x security, you must have the following:

- An authentication server (RADIUS server), which is software that is installed on a PC or server on your network or an EAS. The authentication server accepts or rejects requests from end devices that want to communicate with the 802.1x-enabled network. For help, see Chapter 7, “Configuring the Embedded Authentication Server (EAS)” on page 204.
- An authenticator, which is an access point on your network. The authenticator receives requests from end devices that want to communicate with the network and forwards these requests to the authentication server. The authenticator also distributes the WEP keys to end devices that are communicating with it.
- End devices that are 802.1x-enabled. These end devices have an 802.11b or an 802.11a radio and a supplicant (EAP-TLS, EAP-TTLS or PEAP) loaded on them. Supplicants request communication with the authenticator using a specific EAP authentication type. For more information on the availability of 802.1x-enabled end devices, contact your local Allied Telesyn representative.
- A trusted certificate authority (CA), which issues digital authentication certificates. Allied Telesyn and others can provide the service of acting as a CA and can issue certificates. For more information, contact your local Allied Telesyn representative.
- The authentication server and end devices with supplicants need certificates. A CA certificate is the root certificate or public key. A server certificate (sometimes referred to as the client certificate) is the private key. For more details, see“About Certificates” on page 206.
  - The authentication server must have both a CA certificate and a server certificate installed on it.
  - An end device with an EAP-TTLS supplicant or a child access point using secure IAPP-TTLS needs only the CA certificate.

- Any device with an EAP-TLS supplicant (end device or child access point) needs both the CA certificate and the server certificate.
- If the child access point is using SWAP and is an authenticator, it does not need any certificates loaded on it. Only the authentication server and supplicants need certificates.

If the access point has two radios, or if the access point contains one 802.11g or 802.11a radio with multiple service sets, you can implement 802.1x security on one radio network or both radio networks, as long as the radio supports 802.1x security.

For example, you have an access point with dual 802.11b radios and some end devices that have a supplicant and some end devices that do not have a supplicant. In the access point, you can configure one 802.11b radio to use 802.1x security and the other 802.11b radio to use an ACL.

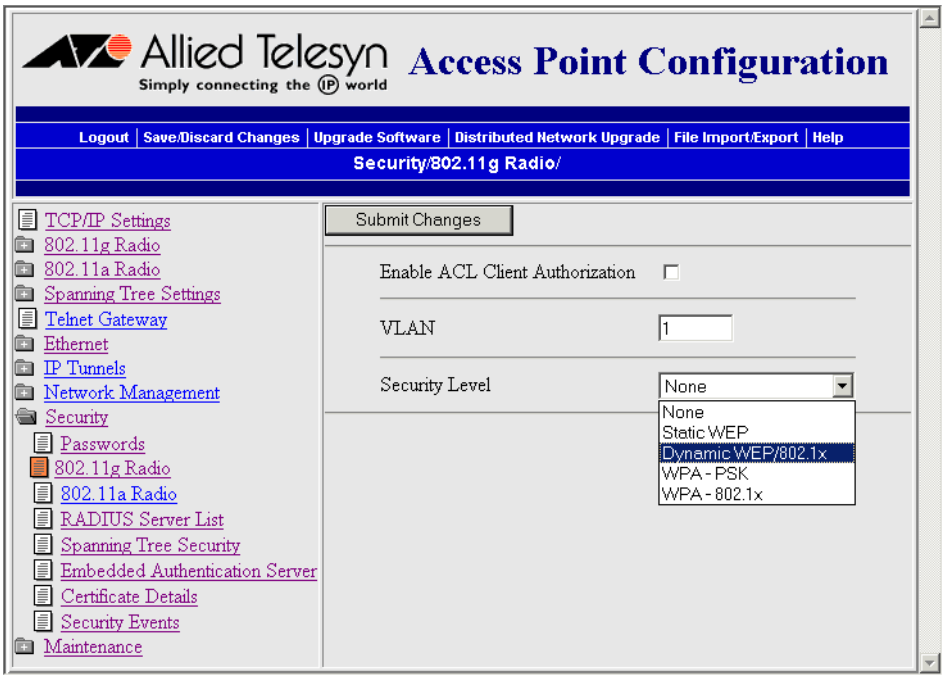
Configuring the Access Point as an Authenticator

The access point, when acting as an authenticator, receives requests from end devices that want to communicate with the network and forwards these requests to the authentication server. It also distributes the WEP keys to end devices that are communicating with it. Before you configure the access point as an authenticator, the access point should be installed and configured to communicate with the wireless end devices.

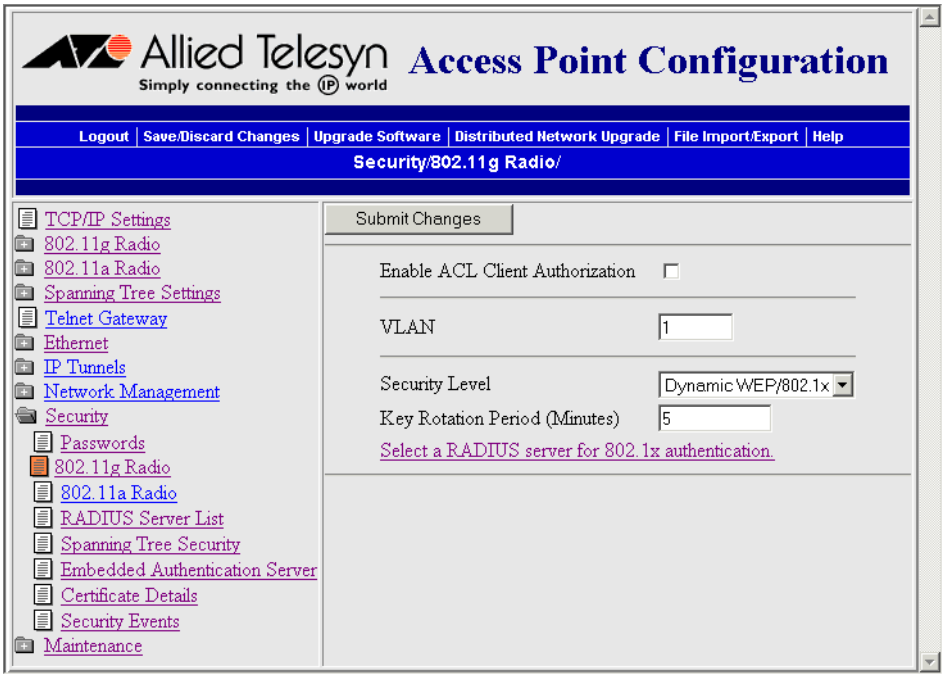
To configure the access point as an authenticator

1. From the main menu, click Security and then click the radio service set that you are configuring. The appropriate radio screen appears.

2. In the Security Level field, select Dynamic WEP/802.1x.



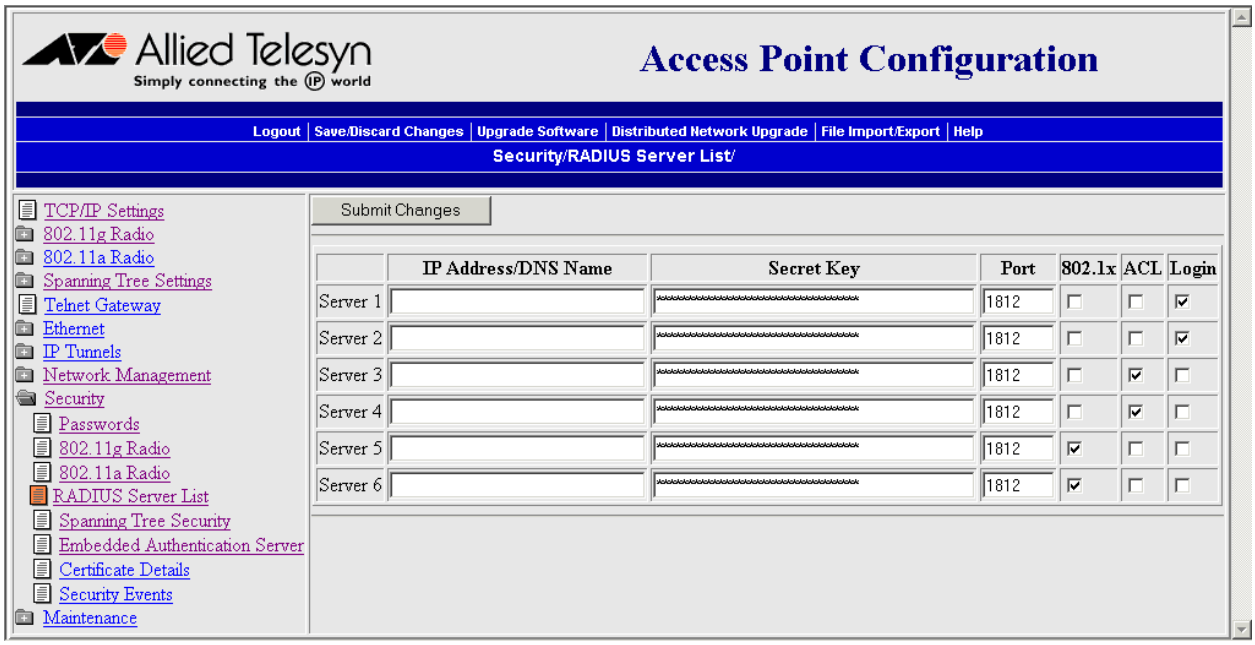
3. Click Submit Changes to save your changes. This screen appears.



4. In the Key Rotation Period (Minutes) field, enter how often (in minutes) the access point generates a new WEP key to distribute to the end devices.

5. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

6. Configure the RADIUS server by clicking Select a RADIUS server for 802.1x authentication. The RADIUS Server List screen appears.



7. For each authentication server, enter the IP address or DNS name, enter the shared secret key, port number, and check the 802.1x check box.

> **Note**
> If you enter more than one authentication server, see page 132 for a description of how the access point uses the servers.

8. Configure the database. Depending on the authentication type, enter the information for each end device that is allowed to communicate with the 802.1x network:

   - In the EAS database, in the Type field choose the authentication type and then enter the information for each end device. For help, see Chapter 7, "Configuring the Embedded Authentication Server (EAS)" on page 204.
   - For help configuring an external RADIUS server, see the documentation that came with your server. You need to enter each authenticator's IP address and the shared secret key. In the database, you need to enter the information for each end device.

Enabling Secure Communications Between Access Points

When you configure a radio to use 802.1x security, you automatically enable spanning tree security, which can be used for both wired access points and WAPs. A secure spanning tree has two functions:

1. To require authentication of any access point attempting to join the spanning tree.

2. To provide encryption of critical Inter-Access Point Protocol (IAPP) frames.

There are three authentication methods that you can use to secure the spanning tree: SWAP, TTLS, or TLS.

When the Access Point Is the Supplicant

By default, TTLS is enabled. If you want to use TTLS, you must also enter a user name and password. This login must match an entry in the authentication server database. When the access point is acting as a supplicant and the authentication server offers the TTLS protocol, the access point sends its user name and password.

You can also enable TLS as the authentication method. You must install a server certificate on each access point that will use this method to authenticate to the network. When the access point is acting as a supplicant and the authentication server offers the TLS protocol, the access point sends its certificate credentials.

If you choose to use both TTLS and TLS, you must choose which protocol the access point offers first and the access point must have a login configured and a server certificate.

By default, Secure Wireless Authentication Protocol (SWAP) is also enabled. The access point tells the authenticator that it can perform SWAP. If the authenticator allows SWAP, SWAP is used. SWAP allows access points to authenticate using an EAP-MD5 challenge. If the supplicant or the authenticator does not allow SWAP, the authentication must happen at the authentication server using TTLS or TLS.

When the Access Point Is the Authenticator

If the Allow SWAP check box is cleared, the access point that is acting as the authenticator will not perform any authentications using SWAP. Supplicants will need to authenticate with the authentication server using TTLS or TLS.

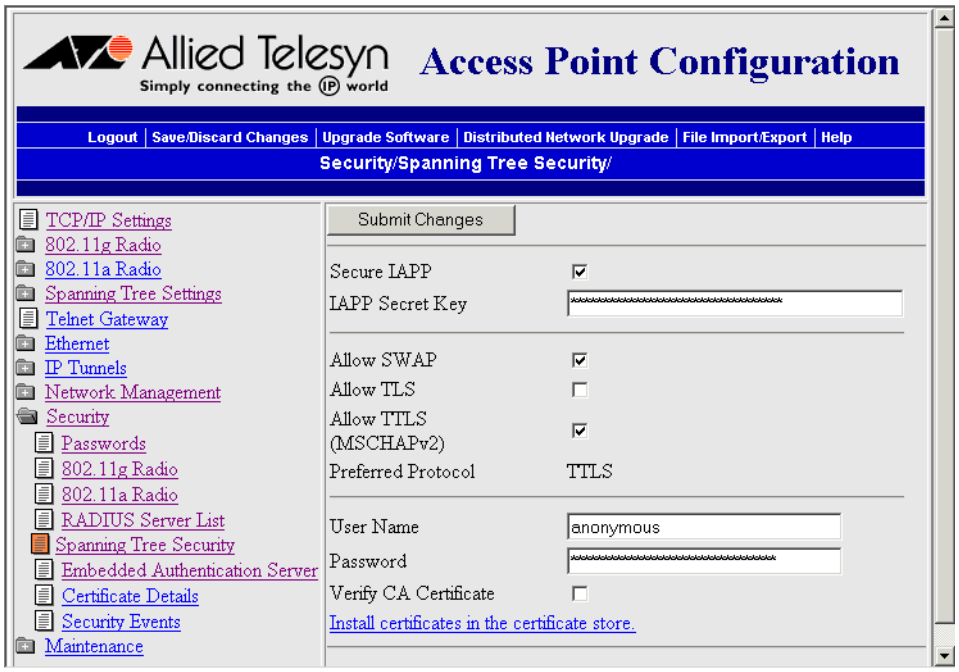
However, older access points do not support these authentication methods. If the Allow SWAP check box is checked, the access point that is acting as the authenticator will authenticate any supplicants that offer

SWAP. Note that SWAP authentication is susceptible to downgrade attacks from rogue supplicants as it is easier to break SWAP than TLS or TTLS.

Configuring Spanning Tree Security

Note
If you are implementing an 802.1x security solution, secure IAPP and secure wireless hops are automatically enabled.

1. From the main menu, click Security > Spanning Tree Security. The Spanning Tree Security screen appears.



2. In the IAPP Secret Key field, enter a secret key. This secret key must be between 16 and 32 bytes.

3. Choose which authentication methods you want to use to authorize the access point to communicate with the network. For help, see the next table.

4. Check the Verify CA Certificate check box and enter the authentication server common names to verify that the access point is connecting to the correct authentication server. Allied Telesyn recommends that you perform this step because it provides another layer of security.

5. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

6. Repeat Steps 1 through 5 for each access point in your spanning tree. All access points must have the same IAPP secret key to communicate with each other.

In the access point that contains the master radio, click Maintenance > AP Connections. The AP Connections screen lists the station radios (including ones in other access points) that are communicating with the master radio. For help, see “Viewing AP Connections” on page 228.

Table 53. Spanning Tree Security–Authentication Method Descriptions

Parameter	Description
Allow SWAP	Determines if this access point authenticates to other access points using SWAP.
Allow TLS	If the authentication server offers the TLS protocol for the authentication method, this check box determines if this access point can use its server certificate to authenticate to the network.
Allow TTLS (MSCHAPv2)	If the authentication server offers the TTLS protocol for the authentication method, this check box determines if this access point uses a login to authenticate to the network. This login must be in the authentication server database.
Preferred Protocol	If TLS and TTLS are enabled, this field specifies which protocol is sent to the authentication server when it sends an unsupported protocol.
User Name	Enter the user name of the access point when it uses TTLS to authenticate to the network.
Password	Enter the password of the access point when it uses TTLS to authenticate to the network.
Verify CA Certificate	Determines if you want to verify that the access point is connected to the correct authentication server. The server certificate signature is verified against the CA certificate and the server common name is verified against the authentication server common names that are configured in the access point.

Configuring Wi-Fi Protected Access (WPA) Security

Wi-Fi Protected Access (WPA) is a strongly enhanced, interoperable Wi-Fi security that addresses many of the vulnerabilities of Wired Equivalent Privacy (WEP). WPA bundles authentication, key management, data encryption, message integrity checks and counter measures in the event of a message attack into one implementation standard.

WPA provides stronger RC4 encryption over standard WEP with the Temporal Key Integrity Protocol (TKIP). In addition, the Michael algorithm provides forgery protection and message integrity. A four-way handshake between the client and access point ensures the reliable and secure distribution of key material needed for encryption and message integrity checks.

Currently, WPA satisfies some of the requirements in the IEEE 802.11i draft standard. When the standard is finalized, WPA will maintain forward compatibility.

WPA runs in Enterprise (802.1x) mode or PSK (pre-shared key) mode:

- In Enterprise mode, WPA provides user authentication using 802.1x authentication and the Extensible Authentication Protocol (EAP). An authentication server (such as a RADIUS server) must authenticate each device before the device can communicate with the wireless network.
- In PSK mode, WPA provides user authentication using a shared secret key between the access point and the end devices. It does not require an authentication server. WPA-PSK is a good solution for small offices or home offices that do not want to use an authentication server.

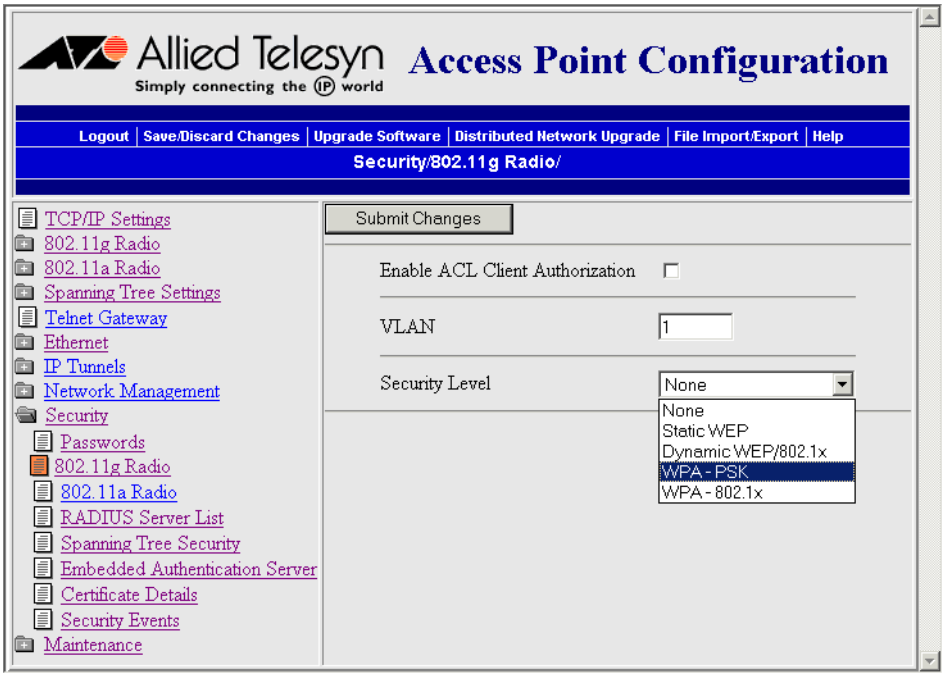
To use WPA security, you need:

- An access point with an 802.11 radio that supports WPA
- End devices with a radio and software that support WPA
- (Enterprise mode only) An authentication server, which is software that is installed on a PC or server on your network or an EAS. The authentication server accepts or rejects requests from end devices that want to communicate with the 802.1x-enabled network. For help, see Chapter 7, "Configuring the Embedded Authentication Server (EAS)" on page 204.

To configure WPA security

1. From the main menu, click Security and then click the radio service set you are configuring. The appropriate radio screen appears.

2. In the Security Level field, choose either WPA - PSK or WPA - 802.1x.



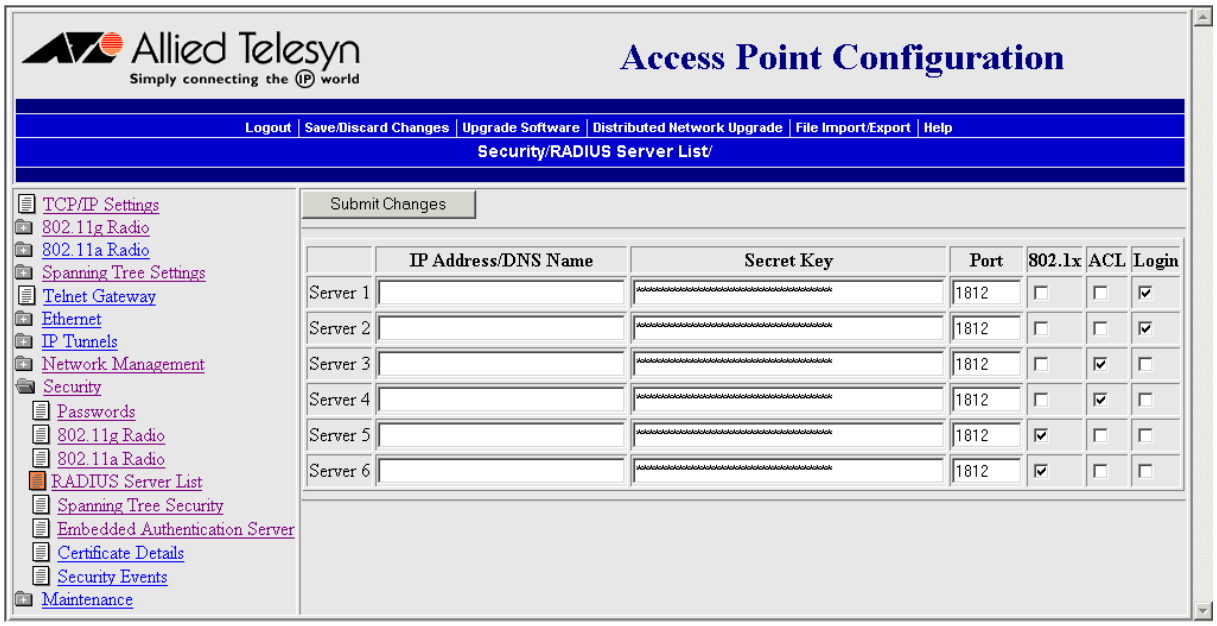
3. Click Submit Changes to save your changes. The screen changes, depending on the security level you choose. For help, see one of the next two screens.

4. Fill in the fields. For help, see one of the next two tables.

5. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

To continue configuring WPA security for WPA – 802.1x mode

1. Configure the RADIUS server by clicking Select a RADIUS server for 802.1x authentication. The RADIUS Server List screen appears.



2. For each authentication server, enter the IP address or DNS name, enter the shared secret key, port number, and check the 802.1x check box.

Note
If you enter more than one authentication server, see page 132 for a description of how the access point uses the servers.

3. Configure the database. Depending on the authentication type, enter the information for each end device that is allowed to communicate with the 802.1x network:

   - In the EAS database, in the Type field choose the authentication type and then enter the information for each end device. For help, see Chapter 7, "Configuring the Embedded Authentication Server (EAS)" on page 204.
   - For help configuring an external RADIUS server, see the documentation that came with your server. You need to enter each authenticator's IP address and the shared secret key. In the database, you need to enter the information for each end device.

Configuring WPA PSK Security

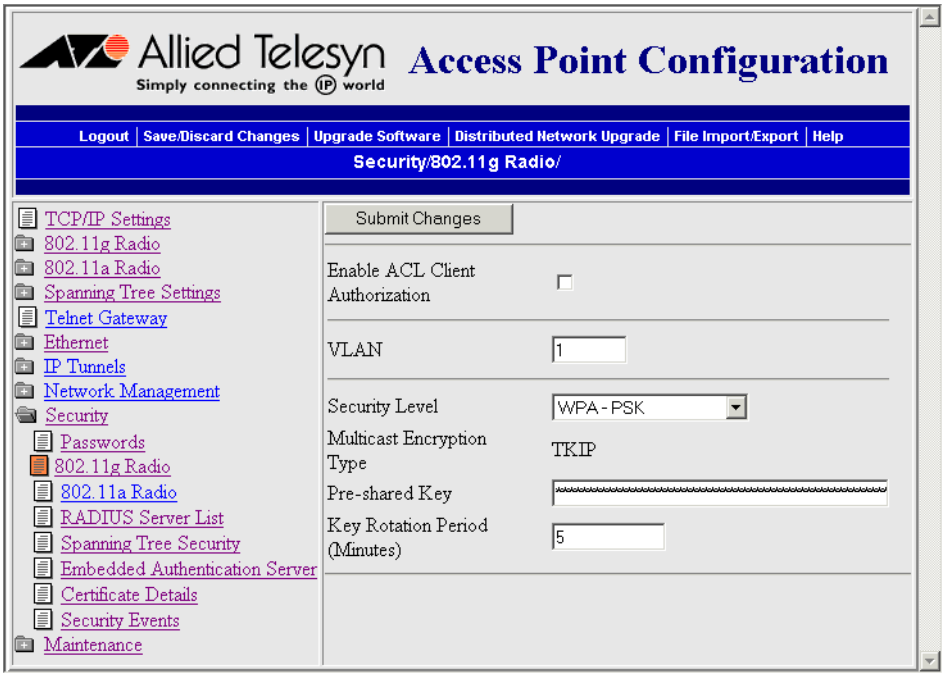


Table 54. WPA PSK Security Parameter Descriptions

Parameter	Explanation
Multicast Encryption Type	Indicates that TKIP is used as the data encryption method for broadcast and multicast for this radio port. A station connected to this port may not select a weaker encryption method to exchange unicast frames.
Pre-shared Key	Allows you to enter the pre-shared key for WPA. You can enter a 256 (32 byte) hexadecimal value or up to a 63 character ASCII passphrase. To enter a hexadecimal key, start the value with 0x and follow it with 64 hexadecimal digits. If you omit the 0x, the value is treated as an ASCII pass-phrase and the key is derived from the pass-phrase using the PBKDF2 algorithm. A short PSK is not as secure as a long PSK.
Key Rotation Period (Minutes)	Allows you to specify the key rotation policy for encryption keys when using WEP in 802.1x and for TKIP group keys when using WPA. The value represents key duration in minutes. The default value is 5 minutes.

Configuring WPA 802.1x Security

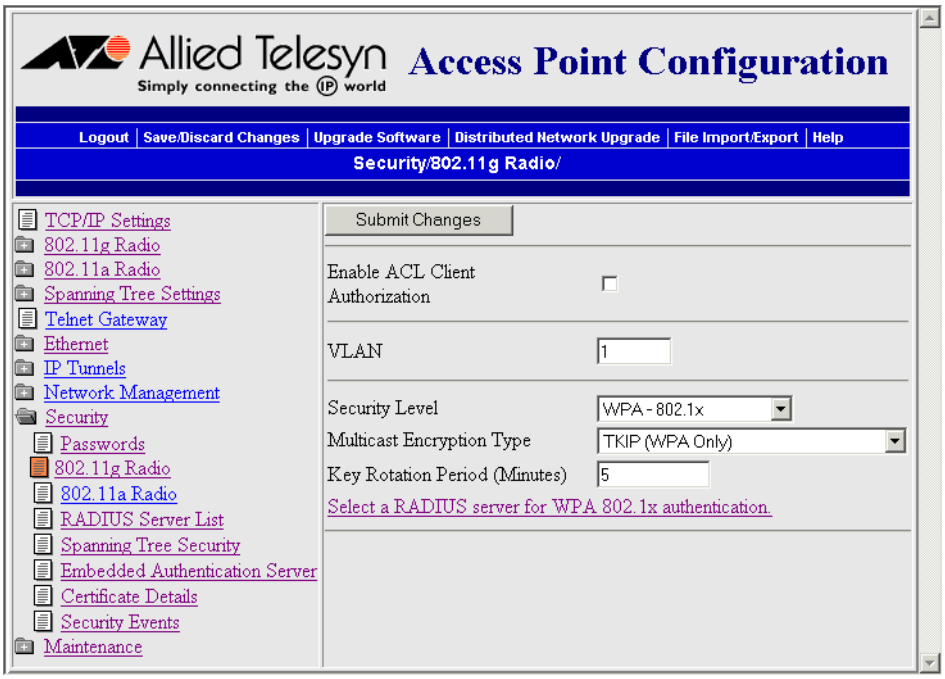


Table 55. WPA 802.1x Security Parameter Descriptions

Parameter	Explanation
Multicast Encryption Type	Allows you to select the data encryption method for broadcast and multicast for this radio port. A station connected to this port may not select a weaker encryption method to exchange unicast frames.
Key Rotation Period (Minutes)	Allows you to specify the key rotation policy for encryption keys when using WEP in 802.1x and for TKIP group keys when using WPA. The value represents key duration in minutes. The default value is 5 minutes.

Chapter 7

Configuring the Embedded Authentication Server (EAS)

This chapter explains how to configure the embedded authentication server (EAS) in your access point for different security solutions to ensure that you have a secure wireless network. This chapter covers these topics:

About the Embedded Authentication Server (EAS)

The AT-WA7500 and AT-WA7501 access points have an embedded authentication server (EAS), which is an internal RADIUS server. In your network, you can use the EAS on any access point. The EAS can act as:

- a password server that maintains a list of logins of users who can configure and manage the access point.
- a RADIUS server that maintains an ACL, which is a list of MAC addresses that can connect to the network.
- a RADIUS server that maintains a list of RADIUS clients (usually access points) that are authorized to connect to the network.
- a RADIUS server that authorizes TLS, TTLS, and PEAP clients to connect to the network.

If you use the EAS, you may not need to buy an external RADIUS server. An EAS supports up to 128 database entries. If you need more database entries, you may be able to use the EAS on different access points for different purposes. For example, you can use the EAS on one access point as a password server and another EAS on another access point as the authentication server.

This table lists the maximum number of end devices that an EAS supports if you turn on the end devices at the same time. However, if you turn on the end devices in groups, the EAS supports 128 clients with unique security credentials.

Table 56. Maximum Number of Simultaneous Authentications Supported

Type of RADIUS Server	Maximum Authentications
Password server	128
ACL authentication server	128
802.1x authentication server	60

About Certificates

Certificates encrypt communication between the internal RADIUS server, RADIUS clients, and the supplicants and HTTPS clients.

There are two types of certificates:

- The trusted certificate authority (CA) certificate (commonly referred to as the “root certificate” or “root cert”) is the public key. Trusted CA certificates can be in *.PEM format or *.CER format. They can contain several trusted CAs but should be kept to a maximum file size of 2Kb.
- The server certificate (sometimes referred to as the client certificate) is the private key. Server certificates can be in either PKCS12 (*.P12/ *.PFX) or *.PEM format.

Understanding Which Access Points Need Certificates

The next table summarizes when an access point needs to have a CA certificate and/or a server certificate installed on it.

Table 57. Access Points and Certificates

Access Point	CA Certificate Needed	Server Certificate Needed
If you want to use the secure web browser (HTTPS) on this access point	No	Yes
If this access point is an authentication server in your 802.1x-enabled network	Yes	Yes
If this access point is a supplicant EAP-TTLS client	Yes	No
If this access point is a supplicant EAP-TLS client	Yes	Yes
If this access point is a backup RADIUS server	No	Yes
If the child access point is using SWAP and is an authenticator access point	No	No

Understanding Which Certificates Are Installed by Default

Your access point comes from the factory with a unique server certificate with a unique common name and passphrase. It also comes with a trusted CA certificate that supports clients running the TLS authentication type. These certificates support the secure web browser interface and provide basic security for all authentication types.

Allied Telesyn can provide the service of acting as a certificate authority and can issue certificates. For more information, contact your local ATI

representative. Or you can install certificates from a third-party certificate authority.

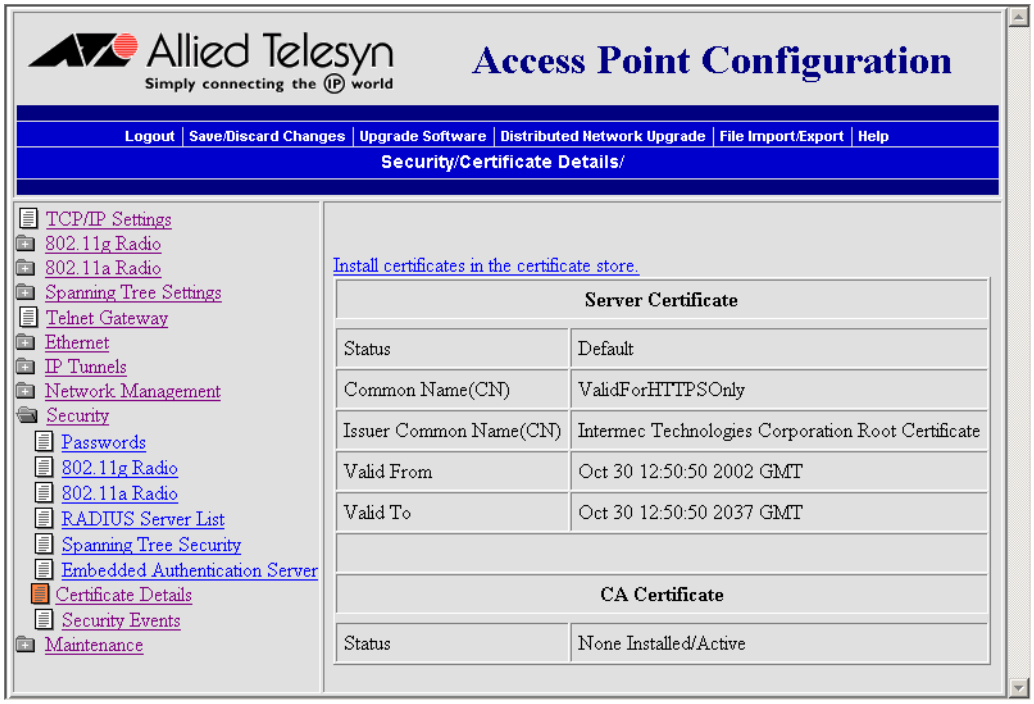
> **Note**
> Access points also come with a default server certificate (ValidforHTTPSOnly). This default certificate supports the secure web browser interface and provides basic security for clients running the TTLS authentication type. As described in the previous section, you may also need a trusted CA certificate and/or a unique server certificate, depending on how you use the access point.

Viewing the Certificates Installed on an Access Point

You can view the Certificate Details screen to determine which certificates are installed on the access point.

To view the certificates

- From the main menu, click Security > Certificate Details. The Certificate Details screen appears.



The Server Certificate table lists the server certificate that is installed, and the CA Certificate table lists the trusted CA certificate that is installed.

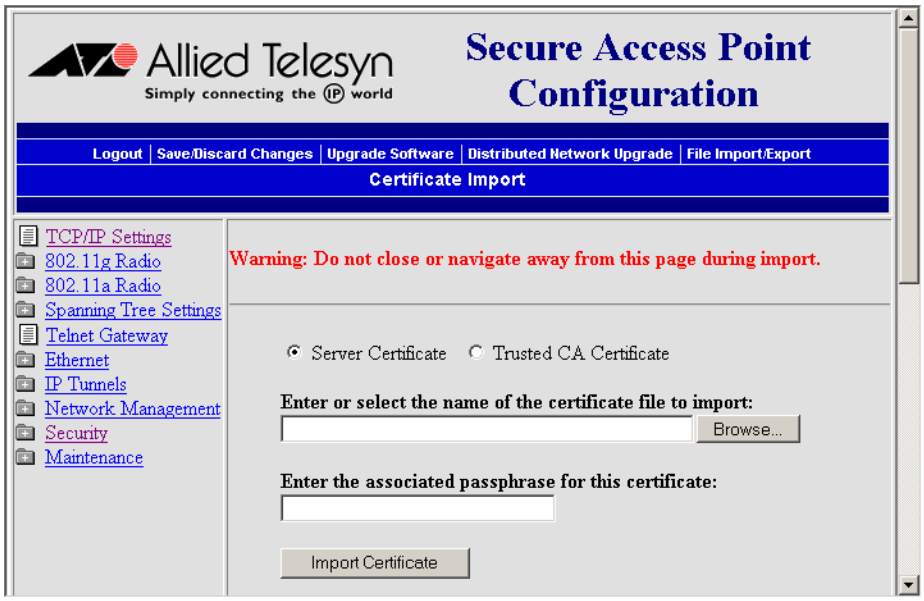
Installing and Uninstalling Certificates

Once you have determined that you need to install a certificate, use this procedure.

To install certificates

1. From the main menu, click Security > Certificate Details. The Certificate Details screen appears.
2. Click Install certificates in the certificate store. The Import Certificate screen appears.

Note
If you are not using the secure web browser, you will be prompted to log in again. Click A secure session is available and log in to the access point. If a Security Alert dialog box appears, click Yes to proceed. Repeat Steps 1 and 2.



3. Click Server Certificate or Trusted CA Certificate.
4. In the Enter or select the name of the certificate file to import field, enter the path and filename of the server certificate. Or click Browse to locate the certificate.
5. (Server Certificate only) In the Enter the associated passphrase for this certificate field, carefully enter the passphrase for the certificate.
6. Click Import Certificate.

To uninstall all certificates

Note
If you follow the procedure to uninstall all certificates, you will lose the unique server certificate and the trusted CA certificate. You will need to contact your local Allied Telesyn representative to purchase new certificates.

1. From the main menu, click Security > Certificate Details. The Certificate Details screen appears.
2. Click Uninstall All Certificates. The unique server certificate and the trusted CA certificate are deleted.

You can still use the secure web browser interface and install new certificates using the default certificate (ValidforHTTPSOnly).

Configuring the EAS

Once you decide which access point will be configured to use its EAS, you need to enable the EAS on that access point and configure its database.

To configure the EAS

1. Install any certificates. For help, see “Installing and Uninstalling Certificates” on page 208.
2. On the access point that will contain the EAS, enable the EAS. For help, see “Enabling the EAS” in the next section.
3. Configure the EAS database. For help, see “Configuring the Database” on page 212.
4. Make sure that all access points that are using this EAS (as a password server, ACL, authentication server, etc.) are configured with this access point’s IP address in the appropriate RADIUS server IP Address field. For help, see:
   - “Configuring the Access Point to Use a Password Server” on page 177.
   - “Using an Access Control List (ACL)” on page 184.
   - “Configuring the Access Point as an Authenticator” on page 193.

Enabling the EAS

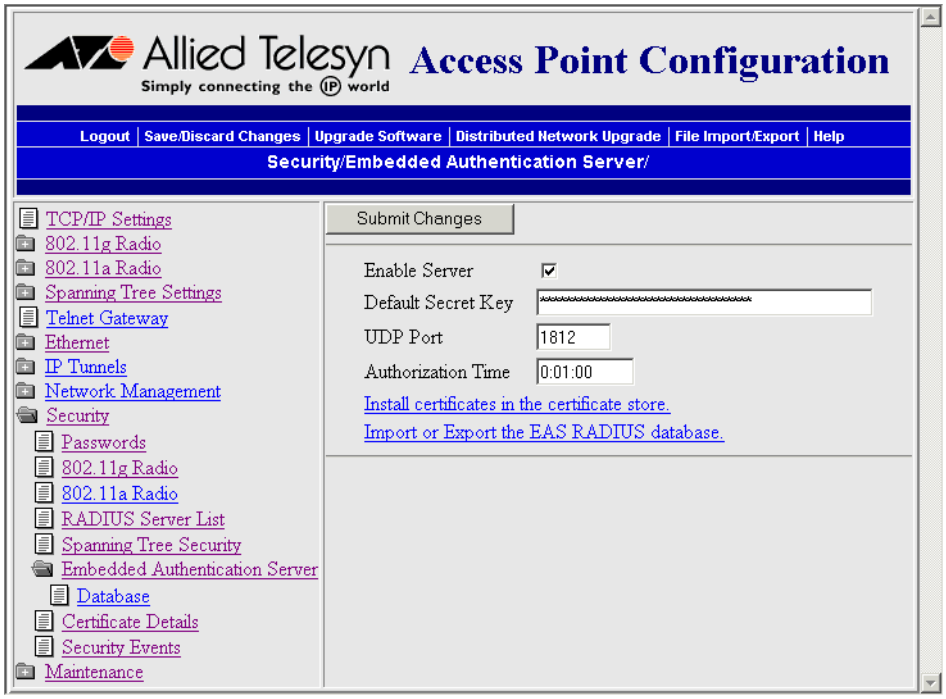
In both AT-WA7500 and AT-WA7501 access points, the default secret key is the same. By having the same default secret key, you can verify that all access points can communicate with the EAS. Then, for more security, you should change the secret key to prevent unauthorized access points from communicating with your network.

If you want to use the same secret key for communications between the EAS and all access points, in the Embedded Authentication Server screen, enter the default secret key. For each access point, in the RADIUS Server List screen, enter the EAS IP address, enter the default secret key and check the 802.1x check box.

If you want to use a different secret key for communications between the EAS and each access point, you need to add each access point to the EAS database as a RADIUS client. For each access point, in the RADIUS Server List, enter the EAS IP address, enter the secret key and check the 802.1x check box.

To enable the EAS

1. Log in to the access point whose EAS you are enabling.
2. From the main menu, click Security > Embedded Authentication Server. The Embedded Authentication Server screen appears.
3. Check the Enable Server check box.
4. Click Submit Changes to save your changes.



5. Configure the parameters. For help, see the next table.
6. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Table 58. EAS Parameter Descriptions

Parameter	Explanation
Enable Server	Determines if you are using a password server to authenticate end devices that can communicate with this access point. Clear this check box.
Default Secret Key	Enter a default secret key that is used between the EAS and all access points. This secret key can be from 1 to 32 characters in ASCII or in hexadecimal. To enter a hexadecimal key, it must start with 0x.
UDP Port	Enter the UDP port number on which the EAS listens. Port number assignments are administered by the Internet Assigned Number Authority (IANA). If you change this value you should choose a number between 49152 and 65535.
Authorization Time	Enter the amount of time that RADIUS clients (access points) remain authorized by the server before they need to be reauthorized. The format is d:hh:mm, where d is days, hh is hours, and mm is minutes. If you enter zeros, the RADIUS server will only authenticate a RADIUS client the first time it connects.
Enable PEAP Fast Reconnect	Determines if PEAP clients can perform a fast reconnect when roaming. Some Microsoft Windows CE supplicants do not support fast reconnect so this option must be disabled to allow them to authenticate.

Configuring the Database

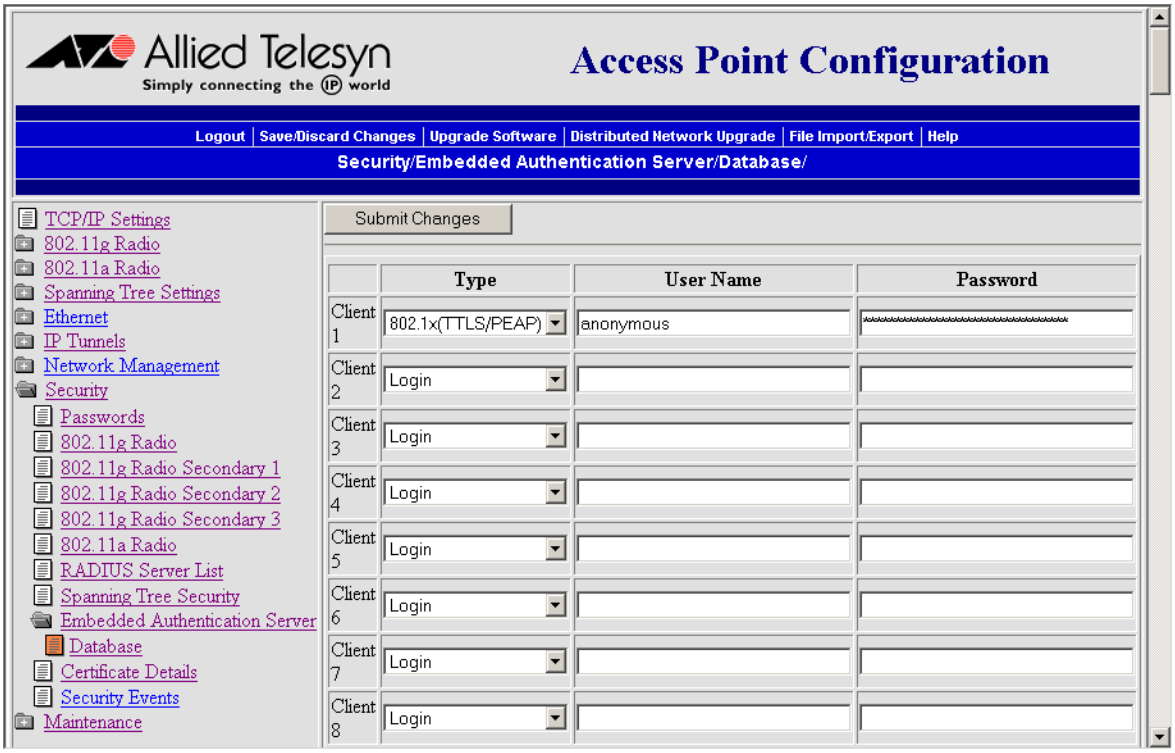
The EAS database contains up to 128 clients that this access point authorizes for logins, RADIUS clients, ACL clients, and 802.1x clients. This screen is hot settable; that is, to activate a change, you click Save/ Discard changes, and then click Save Changes without Reboot.

You can also create a database (using Microsoft Excel or Notepad) and then import it. Or you can configure one database, export it, and import it to an EAS in another RADIUS server. For help, see “Exporting and Importing Databases” on page 217.

Note
Allied Telesyn recommends that when you are done configuring the database, you export it and save the file in a safe place. If you restore the access point to its default configuration, the database is not saved. For help, see "Exporting and Importing Databases" on page 217.

To configure the database

1. Log in to the access point whose EAS you are using.
2. From the main menu, click Security > Embedded Authentication Server > Database. The Database screen appears.



3. In the Type field, choose the type of client you are entering in the database. For help, see the next table.
4. Click Submit Changes to save your changes.
5. Enter the appropriate user name and password, if applicable. User names and passwords can be from 1 to 32 characters. For help, see the next table.
6. Click Submit Changes to save your changes.
7. Repeat Steps 3 through 6 for each client.

8. Click Save/Discard changes, and then click Save Changes without Reboot.

Table 59. Embedded Authentication Server Entry Descriptions

Type Field	Description	User Name Field	Password Field
Login	Enter user names and passwords for users who are authorized to configure and maintain access points using the password server. If you enabled the alternative method ACL, enter the MAC address in the username and password field (no punctuation) for all end devices that are authorized to communicate with the network.	User name	User password
RADIUS	Enter an IP address/DNS name and secret key that is shared by the RADIUS client (access point) and the RADIUS server. You do not need to enter any RADIUS clients if you do not change the default secret key. For more security, you should change the default secret key.	RADIUS client IP address or DNS name	Secret key
ACL	Enter the end device radio MAC address for all end devices that are authorized to communicate with the network.	MAC address	None

Table 59. Embedded Authentication Server Entry Descriptions (Continued)

Type Field	Description	User Name Field	Password Field
802.1x (TTLS/ PEAP)	Enter the login name and password of all end devices that are authorized to communicate with the 802.1x-enabled network. For more security, you should delete the user name "anonymous" and the password "anonymous."	End device login name	End device login password
802.1x (TLS)	Enter the client certificate common name of all end devices that are authorized to communicate with the 802.1x-enabled network.	Client certificate common name	None

Using the Rejected List

The Rejected List screen displays the users and devices that have been rejected by the EAS. You can use this list to discover which users and devices may need to be added to the database. When using the web browser interface, you can immediately add previously rejected end devices to the database. You do not need to click Submit Changes or reboot the access point.

Note
When you reboot the access point, the rejected list is cleared.

To view the rejected list

1. Log in to the access point whose EAS you are using.
2. From the main menu, click Security > Embedded Authentication Server > Rejected List. The Rejected List screen appears.
3. Determine which users and devices you need to add to the database. For help understanding the list, see the next table.

4. Add users and devices to the database. For help see “Adding Entries to the Database” on page 216.

Table 60. Rejected List Values

Column	Description
Type	Lists the type of authentication that failed. The type can be: Login, ACL, TTLS/PAP, TTLS/CHAP, TTLS/EAP, TTLS/MSCHAP, TTLS/MSCHAP-V2, PEAP/MSCHAP-V2, PEAP/GTC, or TLS.
User Name	Lists the value that was passed in the User Name field of the RADIUS server database during the failed attempt.
Last Time	Indicates how long ago the last authentication was attempted.
Count	Indicates how many times the authentication failed.
NAS IP Address	Displays the IP address of the RADIUS server that rejected the client.

Adding Entries to the Database

When you accept TTLS/PAP and PEAP/GTC entries, they are added to the database and require no further configuration.

If the authentication type does not allow the EAS to learn the password of the rejected client (such as TTLS/CHAP), only the user name is added to the database. You need to manually enter the password into the database, click Submit Changes > Save/Discard Changes > Save Changes without Reboot.

To add all entries to the database

1. Click Select All Entries. A check box appears next to all entries.
2. Click Accept Selected Entries.

To add one entry to the database

1. Check the check box next to the entry you want to add to the database.
2. Click Accept Selected Entries.

Clearing the Rejected List

To clear the rejected list, you can either reboot the access point or perform these steps.

1. Click Select All Entries. A check box appears next to all entries.
2. Click Clear Selected Entries.

Exporting and Importing Databases

Note
Allied Telesyn recommends that you use the secure web browser interface (HTTPS) when you export and import databases. Otherwise, the information in the databases is sent in the clear.

The EAS database is simply a comma-separated text file. You can create the database offline (using Microsoft Excel or Notepad) and then import it. The file must have the following format:

```
ACL, 11-22-33-44-55-66
TTLS, username, password
TLS, commonname
LOGIN, username, password
RADIUS, 0.0.0.0, secretkey
```

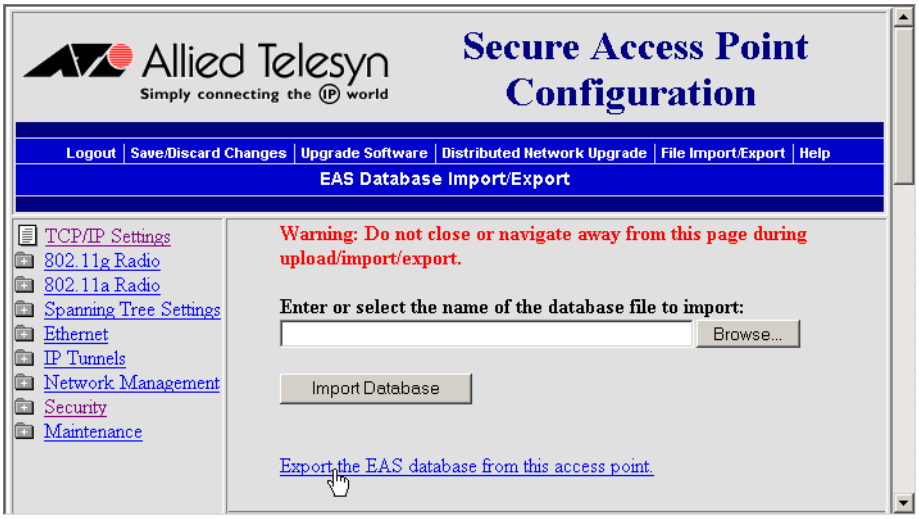
Note
PEAP entries are imported and exported as TTLS entries, since they require the same parameters.

You should export the database so you have a backup version. You may also want to create the database in the primary RADIUS server, and then export it to a file that you can import to a backup RADIUS server.

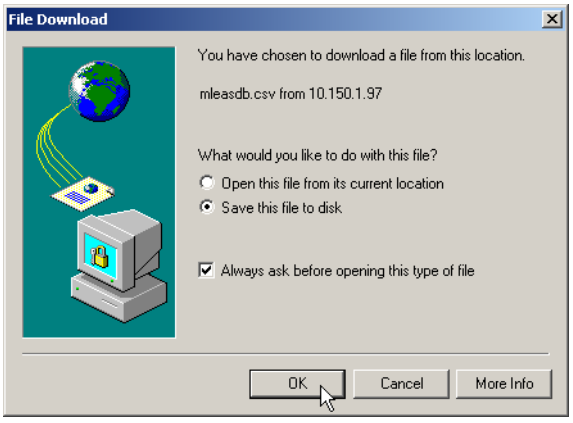
To export a database

1. Log in to the access point whose EAS you are using.
2. From the menu bar, click File Import/Export > Read or write the EAS RADIUS database. The EAS Database Import/Export screen appears.

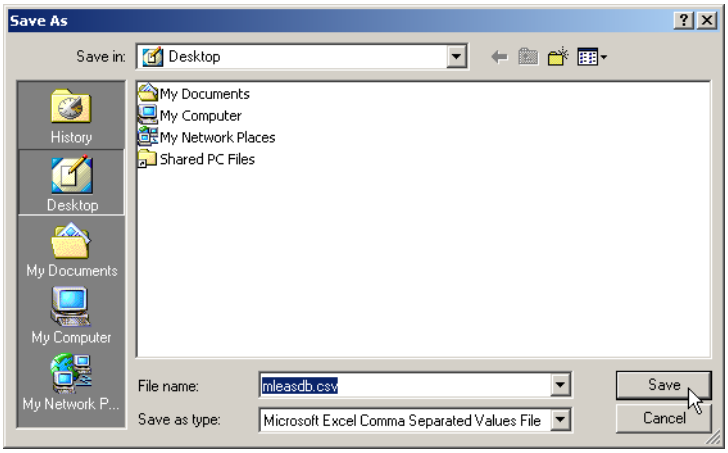
3. If you are not using the secure web browser, click “A secure session is available.” Repeat Steps 1 and 2.



4. Click Export the EAS database from this access point. A File Download dialog box appears.



5. Make sure Save this file to disk is selected, and then click OK. The Save As dialog box appears.



6. Choose the location and filename of the database. If you use the *.CSV extension, you can import it into Microsoft Excel, which recognizes it as a comma separated text file.

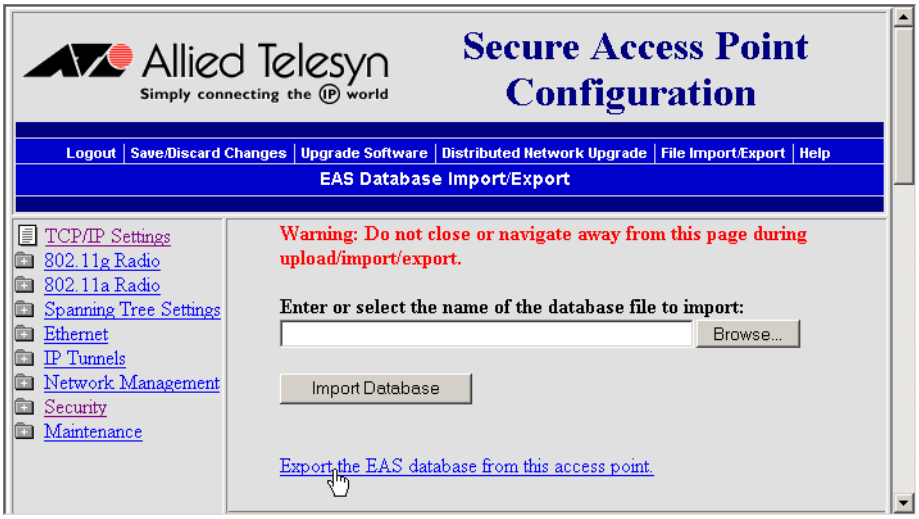
7. Click Save.

To import a database

Note
As soon as you import the database, it is active.

1. Log in to the access point whose EAS you are using.

2. From the menu bar, click File Import/Export > Read or write the EAS RADIUS database. The EAS Database Import/Export screen appears.



3. If you are not using the secure web browser, click A secure session is available. Repeat Steps 1 and 2.

4. Enter the path and filename of the database. Or click Browse to locate the file.

5. Click Import Database.

Chapter 8

Managing, Troubleshooting, and Upgrading Access Points

This chapter explains how to manage, maintain, troubleshoot, and upgrade the access products. This chapter covers these topics:

Managing the Access Points

There are several methods that you can use to manage the access points:

Wavelink Avalanche client management system: You can install the Wavelink Avalanche system to help you manage your wireless network. To use Avalanche, you need Avalanche Manager v3.0 or later. For help, see "Using the Wavelink Avalanche Client Management System" on page 221.

MobileLAN manager: You can purchase this software to make it easy for you to support your wireless network without having expert knowledge of access points or MIBs. It works with the access point's event-driven notification method (instead of traditional polling processes) to maintain real-time status on all access points. It also helps you troubleshoot your network by providing you with multiple views of your network, including what end devices are connected to which access point.

Web browser: For help, see "Using a Web Browser Interface" on page 42.

Communications program (such as HyperTerminal): For help, see "Using a Communications Program" on page 40.

Telnet session: Go to an MS-DOS prompt and type *telnet IPaddress*, where IPaddress has the form x.x.x.x and x is a number from 0 to 255. For more help, see "Using a Communications Program" on page 40. The interface looks similar.

SNMP management station: For help, see "Using Simple Network Management Protocol (SNMP)" on page 226.

Using the Wavelink Avalanche Client Management System

The Wavelink Avalanche client management system uses three main components to help you easily manage your wireless network.

Table 61. Wavelink Avalanche Components

Component	Description
Enabler	Resides on all devices managed by the Avalanche system. It communicates information about the device to the Avalanche Agent and manages software applications on the device.
Agent	Automatically detects and upgrades all devices in the Avalanche system and manages the daily processing functions.

Table 61. Wavelink Avalanche Components (Continued)

Component	Description
Console	The administrative user interface that lets you configure and communicate with the Avalanche Agent. From the console, you can configure and monitor devices and build and install software packages and software collections.

The enabler is already installed on access points with software release 2.0 or later. You can install the agent and the console on the same PC. Avalanche uses a hierarchical file system organized into software packages and software collections:

- Software packages are groups of files for an application that resides on the device.
- Software collections are logical groups of software packages.

For more information about software packages and software collections, see the Wavelink Avalanche documentation and online help. Or, visit the Wavelink web site at www.wavelink.com.

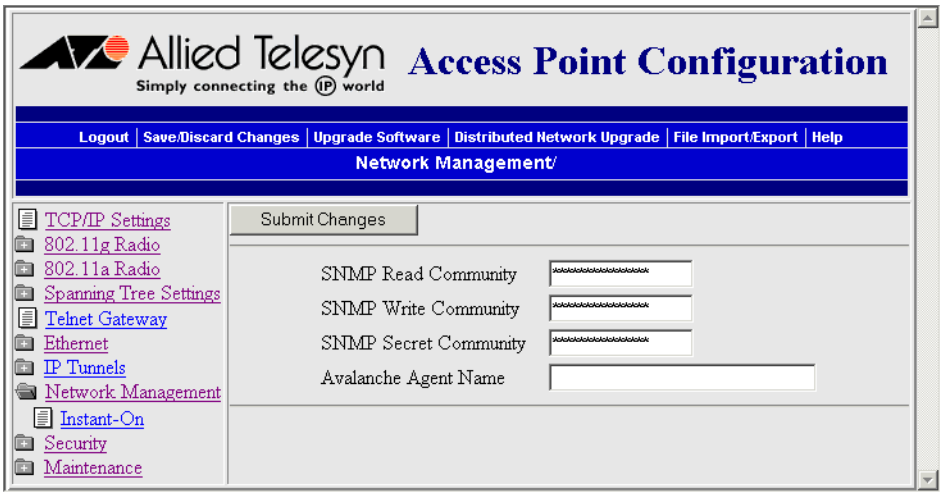
Configuring Your Access Points to Use Avalanche

The first time an access point is assigned an IP address, either manually or from a DHCP server, it attempts to connect to the Avalanche Management Console through the Avalanche Agent. Once it finds the agent, it automatically configures the console IP address.

Note
The access points that you want Avalanche to configure and manage must be on the same subnet as the agent.

To configure your access points to use Avalanche

1. From the main menu, click Network Management. The Network Management page appears.

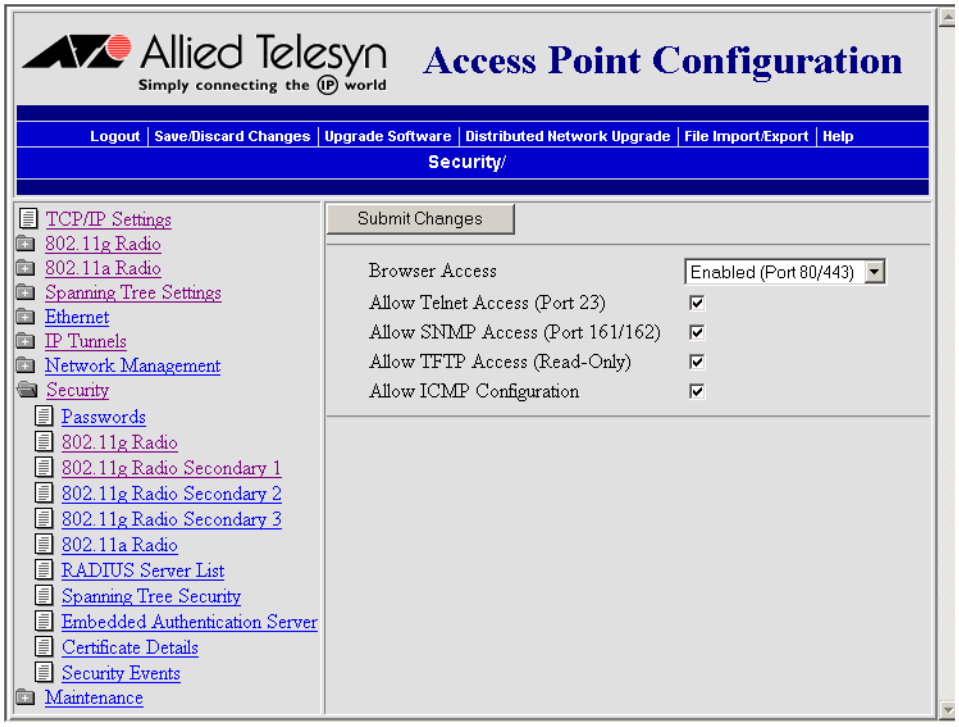


2. In the Avalanche Agent Name field, enter the IP address or DNS name of the console.

   Or, leave this field blank and the access point sends out a broadcast request looking for any available agent.

3. Click Submit Changes to save your changes.

4. From the main menu, click Security. The Security page appears.



5. Verify that the Allow Avalanche Access check box is checked.

6. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see “Saving Configuration Changes” on page 46.

7. Repeat Steps 1 through 6 for each access point.

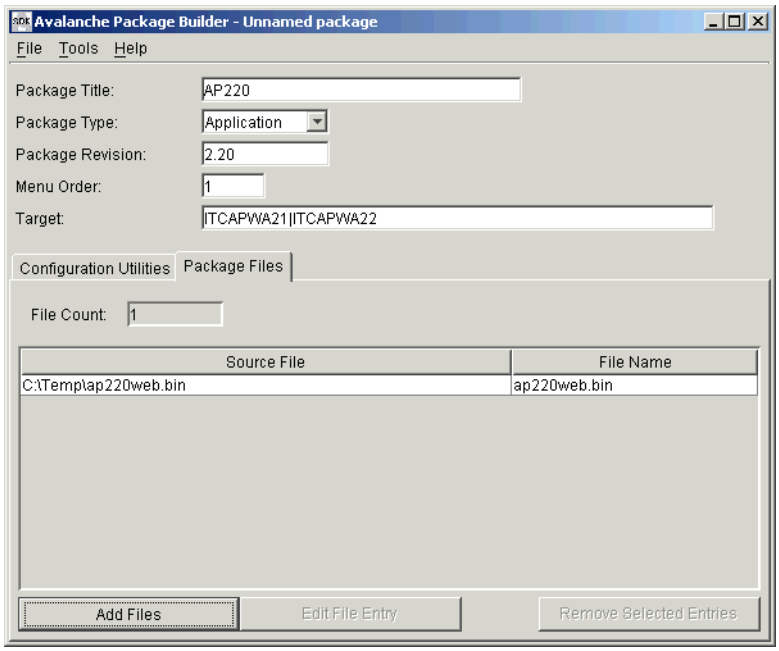
Managing Your Access Points Using Avalanche

Each time the access point is rebooted, it attempts to connect to the Avalanche Agent. When the access point connects to the agent, the agent determines whether an update is available and immediately starts the software upgrade, file transfer, or configuration update. You can also schedule these updates or you can manually initiate an update.

Note
The first time the access point locates the agent, it needs to synchronize with the Avalanche system. On the agent, you must have installed a software package that can be downloaded to the access point.

To use Avalanche to manage your access points

1. On your PC, start Avalanche Package Builder. This screen appears.



2. Create a software package (.AVA file) that includes the latest software release (.BIN file) using Avalanche Package Builder.

3. Install the software package using the Avalanche Management Console.

4. Schedule access point updates or manually initiate an update using the console.

For more information on using the Wavelink Avalanche client management system, see the Wavelink Avalanche documentation and online help. Or, visit the Wavelink web site at www.wavelink.com.

Table 62. Avalanche Parameters

Parameter	Explanation
Package Title	A descriptive title of the application. For example, enter WA7500.
Package Type	Choose Application.
Package Revision	The package version number. For example, enter 2.20.
Menu Order	Enter 1.
Target	Specifies which access points can receive this application. Enter a | between each ModelName. ModelName=ITCAPWA21 ModelName=ITCAPWA22
Package Files	The files that are included in this package. For example, ap220web.bin.

Important Information When Using Avalanche

- If an access point is a DHCP server and Avalanche contains a network profile for the access point that assigns IP addresses from a DHCP server, the access point will lose its static IP address. Any devices that were supposed to receive an IP address from the access point will not succeed.
- If you change security parameters in your wireless network and you are using Avalanche, make sure that you update the security parameters on your end devices before you update the security parameters on your access point. Otherwise, you will lose connectivity between your end devices and your access point.

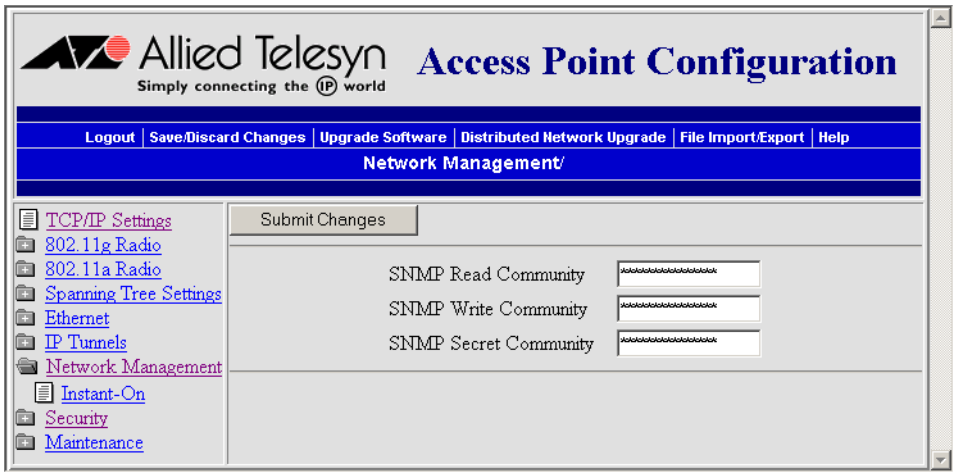
Using Simple Network Management Protocol (SNMP)

The access point can be managed using Simple Network Management Protocol (SNMP); that is, you access the access point from an SNMP management station. Contact your Allied Telesyn representative if you need to obtain a copy of the MIB.

Before you can use an SNMP management station, you must define the access point's SNMP community strings.

To configure the SNMP community strings

1. From the menu, click Network Management. The Network Management screen appears.



2. Configure the SNMP community parameters. For help, see the next table.

3. Click Submit Changes to save your changes. To activate your changes, from the menu bar click Save/Discard Changes, and then click Save Changes and Reboot. For help, see "Saving Configuration Changes" on page 46.

Table 63. SNMP Community Parameter Descriptions

Parameter	Description
SNMP Read Community	Specify a password that provides read-only access. This password can be from 1 to 15 characters and is case sensitive. The default is public.
SNMP Write Community	Specify a password that provides read and write access. This password can be from 1 to 15 characters and is case sensitive. The default is CR52401.

Table 63. SNMP Community Parameter Descriptions (Continued)

Parameter	Description
SNMP Secret Community	Specify a password that provides read and write access and lets the user change the community strings. This password can be from 1 to 15 characters and is case sensitive. The default is Secret.

Maintaining the Access Points

The Maintenance menu lets you view different parameters configured for the access point, including connections, port statistics, and a configuration summary. This information may be needed when you contact Allied Telesyn Technical Support.

You can also view security events that are in the Security Events log, and then you can export them to a file.

Viewing AP Connections

The AP Connections screen shows information about the spanning tree status and the devices connected through the spanning tree.

To view AP connections

- From the menu, click Maintenance > AP Connections. The AP Connections screen appears. For help interpreting the information on this read-only screen, see the next table.

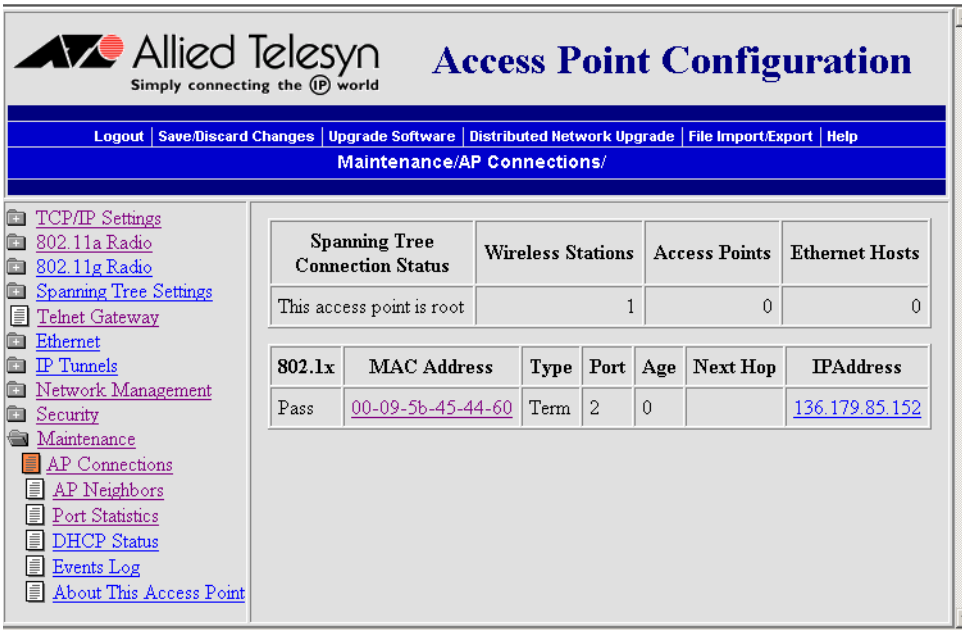


Table 64. AP Connections Screen Fields

Display Field	Description
Spanning Tree Connection Status	Indicates the current status of this access point in relation to the spanning tree: This access point is root: This access point has formed a spanning tree and is serving as root. Connected to root: This access point is participating in a spanning tree as a child directly connected to the root access point. Or, this access point has found a spanning tree and is negotiating with the root access point to join the tree. Connected to non-root: This access point is participating in a spanning tree as a child that is not directly connected to the root. Or, this access point has found a spanning tree and is negotiating with a non-root to join the tree. Not connected: This access point is currently searching for a spanning tree, cannot find a spanning tree, or is unable to form its own spanning tree.
Wireless Stations	Displays the number of devices for which this access point provides connectivity via its radio ports.
Access Points	Displays the number of other access points to which this access point has a direct link in the spanning tree.
Ethernet Hosts	Displays the number of Ethernet devices for which this access point is bridging, if this access point is providing bridging for an IP tunnel or wireless LAN segment via its Ethernet network.
ACL/802.1x	Indicates which devices are passed or blocked if you are using an ACL or 802.1x security. If an access point or WAP is blocked and should be allowed to pass, you need to re-enter the IAPP secret key in both devices.

Table 64. AP Connections Screen Fields (Continued)

Display Field	Description
MAC Address	Shows the address of the connected device. If another access point is connected to this access point, you see the Ethernet MAC address. If a WAP is connected to this access point, you see the radio MAC address. Click the hyperlink to perform a MAC ping or display a radio link statistics screen.
Type	Indicates the nature of the connection: Root/Parent or Parent: Indicates an access point serving as root access point or parent, to which this access point is connected. Pending Root: Indicates that this access point has found a suitable spanning tree and is attempting to join the tree. AP: Indicates an access point linked to this root access point via the Ethernet. AP Wireless: Indicates an access point bridging for a wireless secondary LAN linked to this access point. AP Tunnel: Indicates an access point bridging for an IP tunnel linked to this root access point. AP Remote: Indicates an access point serving as a child on a secondary LAN. Term: Indicates a wireless end device connected to a radio port on this access point. EHost: Indicates a secondary LAN Ethernet device for which this access point provides bridging to the spanning tree.

Table 64. AP Connections Screen Fields (Continued)

Display Field	Description
Port	Displays the port through which the connection is established: E: Ethernet port 1, 1:1, 1:2, or 1:3: First radio slot (primary, secondary 1, secondary 2, or secondary 3). 2, 2:1, 2:2, or 2:3: Second radio slot (primary, secondary 1, secondary 2, or secondary 3). I: IP tunnel port.
Age	Displays the number of minutes since last contact with this device.
Next Hop	Displays the path to the root access point of the spanning tree via this connection.
IP Address	The IP address associated with this device, if discovered by the access point. Click the hyperlink to perform the ICMP Echo ping.

Viewing AP Neighbors

The AP Neighbors screen provides information on all the access points (even hidden access points) in the area. It displays information gathered by the radios receiving beacons from other sources as it operates on a specific channel. You can use this screen to help you:

- distribute channels for maximum wireless network performance.
- identify interference problems.

To view AP neighbors

❒ From the menu, click Maintenance > AP Neighbors. The AP Neighbors screen appears. For help interpreting the information on this read-only screen, see the next table.

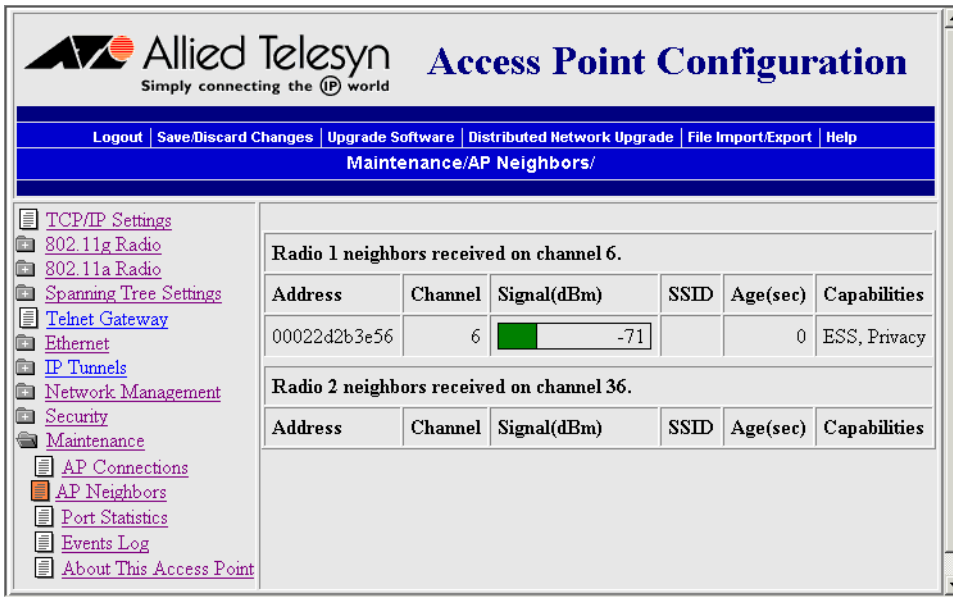


Table 65. AP Neighbors Screen Fields

Display Field	Description
Address	Displays the MAC address of the originator of the contact.
Channel	Displays the channel advertised in the beacon.
Signal (dBm)	Displays the power level of reception measured in dBm. Graph colors red, yellow, green indicate poor, adequate, good signal levels for communication, respectively.
SSID	Displays the SSID advertised in the beacon. This field may or may not be advertised by the originator of the contact.
Age (sec)	Displays the amount of time in seconds that has elapsed since the last contact from the originator.

Table 65. AP Neighbors Screen Fields (Continued)

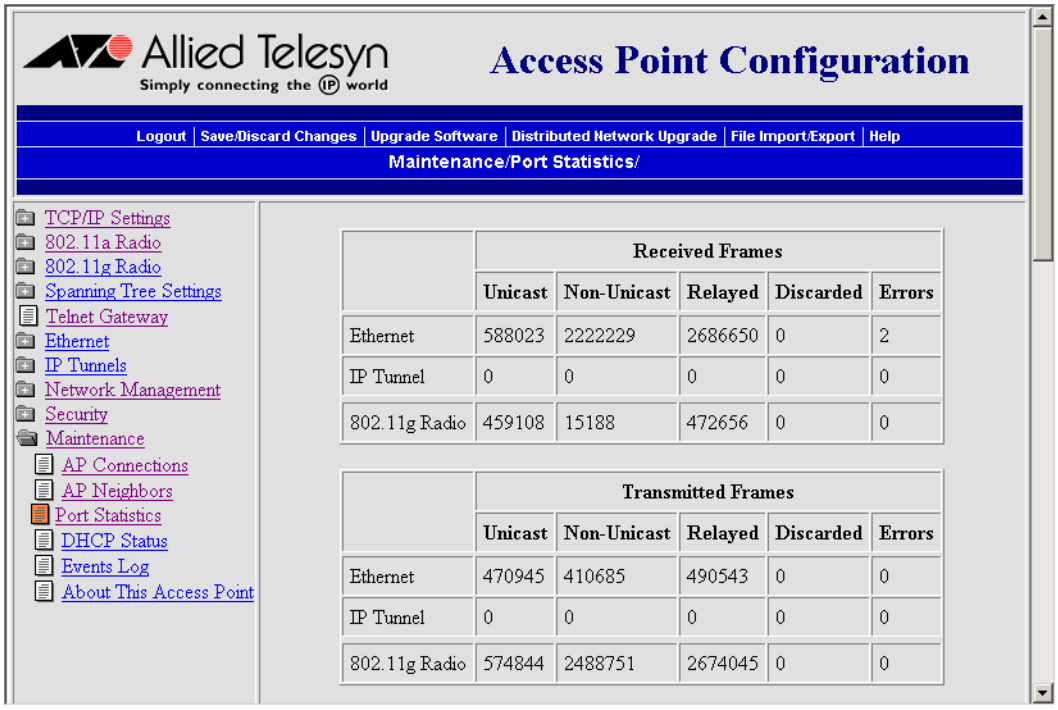
Display Field	Description
Capabilities	This information is derived from the capability information sent in the beacon. Capabilities may include: ESS: Set for an access point and cleared for an end device or ad-hoc device. IBSS: Cleared for an access point and set for an end device or ad-hoc device. Privacy: Indicates that encryption is required on this service set. Short Preamble: Indicates that short preambles may be used for frame transmission on this service set. OFDM Allowed: Use of DSSS-OFDM is allowed within this BSS. Short Slot: Indicates that short slot timing is being used on this service set. If this field is not present, then longer slot timing is being used for backward compatibility. CFPoll: Access point uses point coordination function for delivery and polling. CFReq: Access point uses point coordination function for delivery but does not support polling.

Viewing Port Statistics

The Port Statistics screen shows the total number of frames and bytes that the access point has received and transmitted since it was last booted. You can also view graphs of inbound and outbound packets for the port.

To view port statistics

- From the menu, click Maintenance > Port Statistics. The Port Statistics screen appears. This screen is read-only.



	Received Frames				
	Unicast	Non-Unicast	Relayed	Discarded	Errors
Ethernet	588023	2222229	2686650	0	2
IP Tunnel	0	0	0	0	0
802.11g Radio	459108	15188	472656	0	0

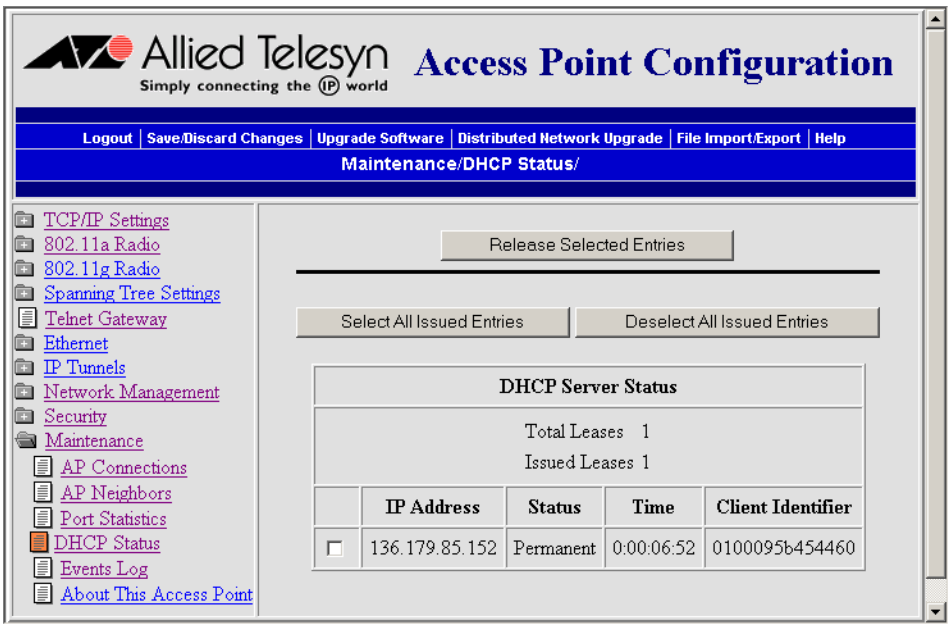
	Transmitted Frames				
	Unicast	Non-Unicast	Relayed	Discarded	Errors
Ethernet	470945	410685	490543	0	0
IP Tunnel	0	0	0	0	0
802.11g Radio	574844	2488751	2674045	0	0

Viewing DHCP Status

The DHCP Status screen shows a status report for the DHCP client or DHCP server. If the access point is a DHCP server and if the Permanently Save IP Address Mappings check box is checked, you can delete entries from the server's permanent address map.

To view DHCP status

- From the menu, click Maintenance > DHCP Status. The DHCP Status screen appears.



Viewing the Events Log

The Events Log screen shows a the events that have been logged by this access point. These events are cleared when the access point loses power or is rebooted.

To view the Events Log

- From the menu, click Maintenance > Events Log. The Events Log screen appears. For help understanding the events on this read-only screen, see the next table.

Table 66. Events Log Description

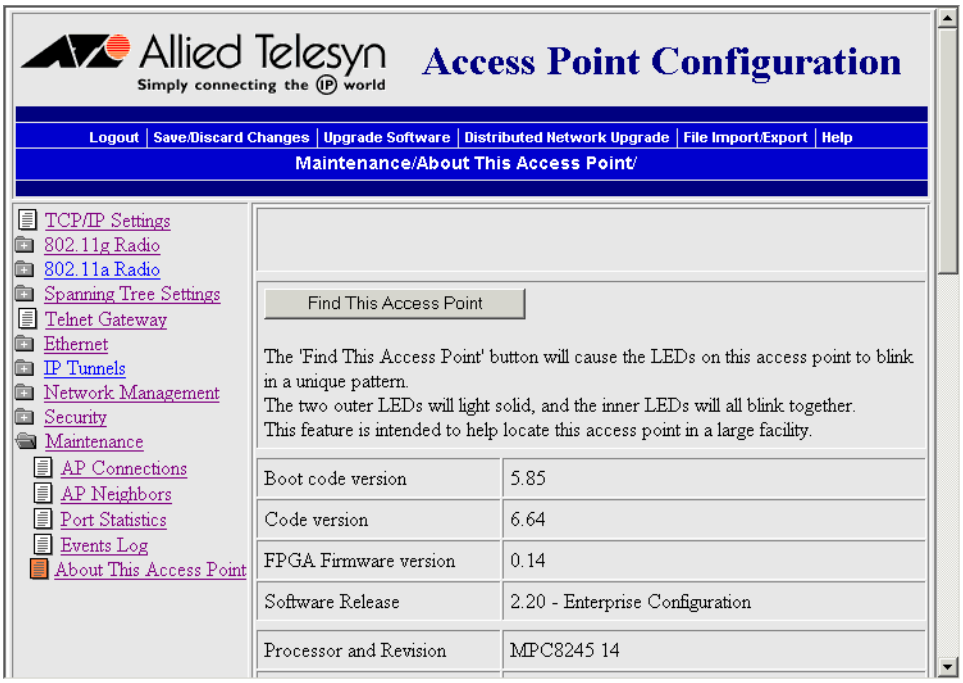
Column	Description
MAC Address	Indicates the Ethernet MAC address of the device that caused the event.
IP Address	Indicates the IP address of the device that caused the event.
Priority	Indicates the priority of the event: Critical, High, Low, and Informative. Critical and High priority events generate an SNMP trap.
Trap?	Indicates whether an SNMP trap is sent for this particular event type.
Count	Indicates the number of times the event occurred.
Type	Indicates a description of the event.
Additional Data	Indicates extra event-specific information.
Age	Indicates the amount of time that has passed since the event occurred.

Viewing the About This Access Point Screen

This screen shows information about the access point, such as the software version, radio versions, and MAC addresses. It also provides a configuration summary section, which can either show you the configuration settings that are different from the factory default settings or it can show you all the configuration settings. Also, you can view a processor utilization graph.

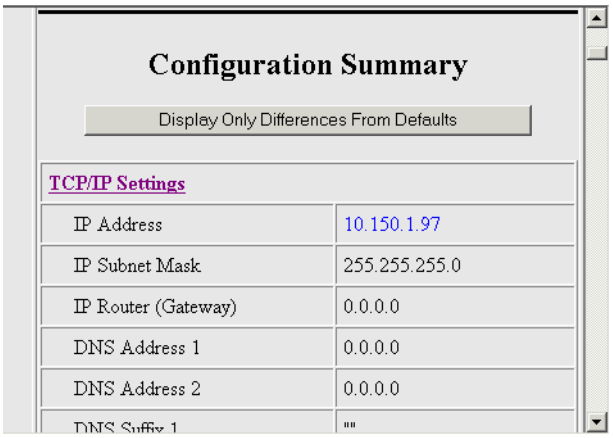
To view About This Access Point

1. From the menu, click Maintenance > About This Access Point. The About This Access Point screen appears. This screen is read-only.



2. Scroll down to view more information about the access point.

3. Continue scrolling down until you see the subtitle Configuration Summary.

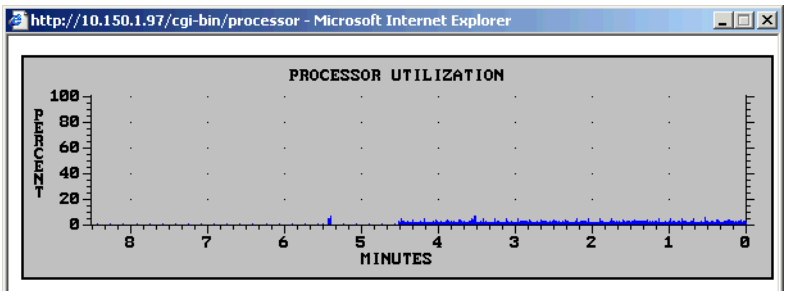


4. Click the button under the Configuration Summary title to switch between displaying all configuration settings and displaying the configuration settings that are different from the factory default settings.

To view a processor utilization graph

1. From the main menu, click Maintenance > About This Access Point. The About This Access Point screen appears. This screen is read-only.

2. Click the Processor and Revision link. The Processor Utilization graph appears.



Using the LEDs to Locate Access Points

You can use the LEDs to help you locate a specific access point in your building.

To locate an access point

1. From the menu, click Maintenance > About this Access Point. The About this Access Point screen appears.

2. Click the Find This Access Point button. The access point LEDs start blinking, as shown in the next table.

Table 67. Find This Access Point

Power	Wireless #1	Wireless #2	Wired LAN	Root/Error
○	☼	☼	☼	○

○ LED On ● LED Off ☼ LED Flashing

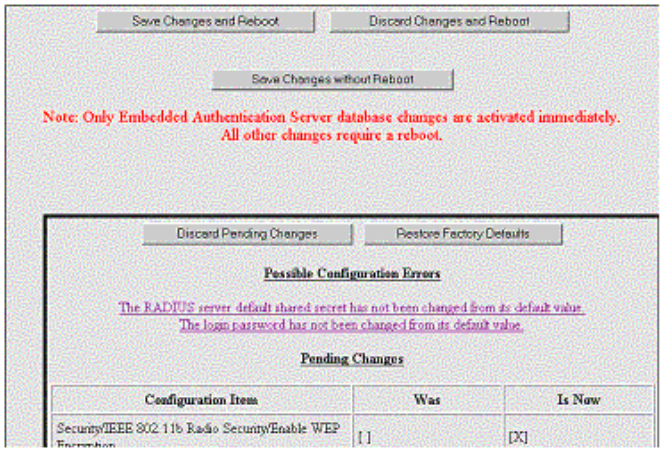
3. The LEDs continue to blink until you click the Finished Finding Access Point button.

Restoring the Access Point to the Default Configuration

You may need to restore the access point to the factory default configuration. For a list of the default settings, see Appendix B, "Default Settings." To restore the access point to the default configuration, you can use the Web browser interface, as explained in the following procedure:

1. In the menu bar, click Save/Discard Changes.

   This screen appears.



2. Click Restore Factory Defaults. Under Pending Changes, you will see a list of what parameters need to be changed.

3. Click Save Changes and Reboot. When the access point is done rebooting, it will use the factory default settings as its active configuration. You may need to reset the IP address and other network parameters.

Troubleshooting the Access Points

This section provides you with information on the installation, configuration, and operation of the access point.

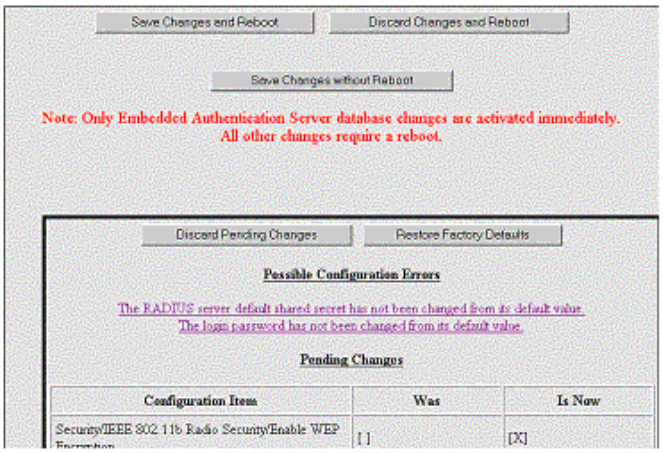
Using the Configuration Error Messages

When you click Save/Discard Changes, the access point checks for potential problems with the network configuration and security settings. The access point displays error messages under the Possible Configuration Errors heading. Each error message is a hyperlink, which you can click to go to the screen where you can fix the possible configuration error.

You can save the configuration changes without resolving any of the possible configuration errors, but the access point may not operate as expected.

Note
The access point can only check its own configuration for possible errors. It cannot check to see if the SSIDs, passwords, shared secret keys, and other settings are all the same or compatible on other devices.

Screen Showing Possible Configuration Errors



To resolve possible configuration errors

1. Using your web browser, click Save/Discard Changes on the menu bar.
2. Review the error messages listed under the Possible Configuration Errors heading.

3. Click each error message to jump to the configuration screen where you can resolve the possible configuration error.

   The configuration error messages are listed in the next table. Most are self explanatory, but a few require additional information.

Table 68. Alphabetized List of Configuration Error Messages

Configuration Error Message	Additional Information
A RADIUS entry in the RADIUS database has a IP address but no secret key (password).	
A RADIUS entry in the RADIUS database has a secret key (password) but no IP address.	
A RADIUS server entry points at this access point but the Embedded Authentication Server is not enabled.	
A RADIUS server entry points at this access point but the shared secret does not match that of the Embedded Authentication Server.	The Default Secret Key for the EAS does not match the secret key value in the RADIUS Server List. For help, see "Enabling the EAS" on page 210.
A RADIUS server entry points at this access point but the UDP port number does not match that of the Embedded Authentication Server.	The UDP port number in the EAS does not match the port number entered in the RADIUS Server List. For help, see "Enabling the EAS" on page 210.
A secure service set is available, but wireless hops are allowed on an insecure service set.	
A username/password entry in the RADIUS database has a password but no username.	
A username/password entry in the RADIUS database has a username but no password.	

Table 68. Alphabetized List of Configuration Error Messages (Continued)

Configuration Error Message	Additional Information
All SSID values must be unique per physical radio.	While configuring multiple service sets, you did not specify a unique SSID (network name) for each service set. For help, see “Configuring the 802.11g Radio” on page 98 or “Configuring the 802.11a Radio” on page 119.
An entry in the RADIUS server list is using a default secret key.	Allied Telesyn recommends that you change the secret key from the default for security reasons.
At least one 802.1x supplicant protocol must be enabled.	
Matching WEP keys will merge VLAN multicast.	
No RADIUS servers have been configured for 802.1x authentication.	Click the message and check the 802.1x check box for at least one server in the RADIUS Server List.
No RADIUS servers have been configured for ACL authorization.	Click the message and check the ACL check box for at least one server in the RADIUS Server List.
No RADIUS servers have been configured for login authorization.	Click the message and check the Login check box for at least one server in the RADIUS Server List.
The 802.1x username and password have not been changed from their default values.	

Table 68. Alphabetized List of Configuration Error Messages (Continued)

Configuration Error Message	Additional Information
The access point is set to originate IP tunnels but no there are no tunnel IP addresses.	On the IP Tunnels screen, Mode is set to Originate if Root, but no IP addresses have been added to the IP Addresses screen. Either change the mode or add some addresses. For help, see "Configuring IP Tunnels" on page 148 and "Configuring the IP Address List" on page 149.
The address range for the DHCP server is invalid.	On the TCP/IP Settings > DHCP Server Setup screen, the Low Address and High Address are not set correctly. For help, see the Table 16, "DHCP Server Setup Parameter Descriptions" on page 73.
The DHCP server is enabled with an address range that is too large. If saved, the range will be truncated to the maximum number of addresses.	On the TCP/IP Settings > DHCP Server Setup screen, the Low Address and High Address are not set correctly. For help, see the Table 16, "DHCP Server Setup Parameter Descriptions" on page 73.
The DHCP server requires a non-zero IP address.	For help, see "Configuring the Access Point as a DHCP Server" on page 70.
The DHCP server subnet mask is invalid.	For help, see the Table 16, "DHCP Server Setup Parameter Descriptions" on page 73.
The IAPP secret key has not been changed from its default value.	Allied Telesyn recommends that you change the IAPP secret key from the default for security reasons.
The IP Address is zero.	For help, see "Configuring the TCP/IP Settings" on page 65.

Table 68. Alphabetized List of Configuration Error Messages (Continued)

Configuration Error Message	Additional Information
The IP Address and IP Router must share the same subnet.	For help, see “Configuring the TCP/IP Settings” on page 65.
The IP Subnet Mask is invalid.	For help, see “Configuring the TCP/IP Settings” on page 65.
The IP Subnet Mask should not be zero.	For help, see “Configuring the TCP/IP Settings” on page 65.
The login password has not been changed from its default value.	
The RADIUS server shared secret has not been changed from its default value.	
The read-only password has the same value as the read-write password.	
There are TLS entries in the embedded authentication server database but no CA certificate is installed.	You need to install a trusted CA certificate. For help, see “Installing and Uninstalling Certificates” on page 208.
This device is configured as a login RADIUS server but no login database entries exist.	For help, see Table 59, ”Embedded Authentication Server Entry Descriptions” on page 214.
You have elected to verify the server certificate but no CA certificate is installed in the certificate store.	You need to install a trusted CA certificate. For help, see “Installing and Uninstalling Certificates” on page 208.
You have elected to verify the server certificate but the authentication server common name is blank.	
You have enabled Secure Credential Creation for Instant-On, but no 802.1x-enabled RADIUS servers have been selected.	

Table 68. Alphabetized List of Configuration Error Messages (Continued)

Configuration Error Message	Additional Information
You have enabled the embedded authentication server but you have not installed a server certificate to identify this device.	You need to install a server certificate. For help, see "Installing and Uninstalling Certificates" on page 208.
You have enabled TLS authentication but you have not installed a server certificate to identify this device.	You need to install a server certificate. For help, see "Installing and Uninstalling Certificates" on page 208.
You have enabled WPA pre-shared key for a radio port but the pre-shared key for that port is empty.	For help, see the Table 54, "WPA PSK Security Parameter Descriptions" on page 202.

Troubleshooting With the LEDs

When the access point boots, it performs internal diagnostics and the LEDs display the pattern shown in the next table.

Table 69. MobileLAN access LED Boot Sequence for Release 2.2 (or later)

Power	Wireless #1	Wireless #2	Wired LAN	Root/Error	Description
●	●	○	●	●	Checksum Test starts
●	○	○	●	●	Checksum Test fails
○	●	●	●	●	Monitor Load
○	○	○	●	●	PCI Bus Test starts
○	○	●	●	●	PCI Bus Test fails
●	●	●	○	●	RAM Test starts
○	●	○	●	●	RAM Test fails

Table 69. MobileLAN access LED Boot Sequence for Release 2.2 (or later) (Continued)

○	☼	☼	☼	●	Only Boot ROM code is available on access point. Load new files.
	(Wireless #1 and #2 blink in unison.)				

○ LED On ● LED Off ☼ LED Flashing

After the AT-WA7500 or AT-WA7501 successfully boots, the LEDs display one of these patterns:

Table 70. AT-WA7500 and AT-WA7501 Normal LED Pattern After Booting

|				⊘
○	☼ (Blinks for wireless data traffic.)	☼ (Blinks if a radio is installed.)	☼ (Blinks for wired data traffic.)	☼ (Blinks if the AP becomes root.)

General Troubleshooting

Table 71. General Troubleshooting

Problem/Question	Possible Solution/Answer
The Wireless #1, Wireless #2, and/or Wired LAN LEDs are on solid at the end of the boot process.	An error occurred during the booting process. Consult the previous section to determine which test failed. Connect the access point to a PC with an RS-232 cable, reboot the access point, and watch the error messages. The access point may have a hardware problem. Contact Allied Telesyn Technical Support.

Table 71. General Troubleshooting (Continued)

Problem/Question	Possible Solution/Answer
The Power LED is not on.	1.Make sure the power cable is firmly plugged into the AT-WA7501 access point and the power source. Or make sure the Ethernet cable is firmly plugged into the AT-WA7500 access point and the power over Ethernet bridge. 2.Verify that the power injector has power and will work with another access point at the port in question. 3.Make sure all eight wires in the Ethernet cable are connected, or the power over Ethernet option won't work. 4.Unplug the access point, and then plug it back into the power source. After the access point boots, verify that the Power LED remains on. 5.The access point may have a hardware problem. Contact Allied Telesyn Technical Support.
You cannot connect to the access point using the serial port.	1.Verify that you are using a null-modem cable to connect the access point to your terminal or PC. 2.Verify that you are communicating through the correct serial port. 3.Verify that your terminal or PC is set to 9600, N, 8, 1, no flow control. (Verify that the baud rate is not 115200.) 4.Your system may be in autobaud mode. Reboot and press a key once per second until the sign on screen appears.

Table 71. General Troubleshooting (Continued)

Problem/Question	Possible Solution/Answer
You cannot connect to the access point using a web browser.	1.Verify that you are not using a crossover cable if connected to a hub or a switch. Verify that you are using a crossover cable if connected directly to the PC or server. 2.Verify that you did not disable the Browser Access field in the Security screen. 3.If you access the Internet through a proxy server, be sure you have added the IP address of the access point to the Exceptions list. 4.Depending on the security configuration of your network, your PC may need to be located on the same subnet as the access point.
You cannot ping or telnet to an access point.	1.You must set an IP address and subnet mask using a communications program before you can remotely connect to the access point. 2.Verify that you did not disable the Telnet Access field in the Security screen. 3.The access point may have lost its files. For help, see “Recovering a Failed Access Point” on page 258.
The Ping Utility screen does not appear when you click a MAC address or an IP address in the AP Connections screen.	The web browser you are using does not have Java support. Allied Telesyn recommends that you use Internet Explorer v3.0 (or later) or Netscape Communicator v4.0 (or later).
You cannot connect to the access point using MobileLAN manager or another SNMP management station.	Verify that you did not disable the SNMP Access field in the Security screen.

Table 71. General Troubleshooting (Continued)

Problem/Question	Possible Solution/Answer
The end device cannot connect to the network.	❒ From the Maintenance menu, choose AP Connections and verify that the MAC address of your end device appears on your PC screen. If it does not appear, your end device is not communicating with the access point. Check your radio configuration settings. ❒ Verify that the access point is not filtering out the type of traffic you are trying to pass through it.
The end device cannot synch to the access point.	Verify that the end device and the access point have the same SSID (network name) and security.
The end devices are unable to roam from one access point to another.	The switches in your network may not support backward learning. Use data link tunneling to force all wireless traffic through a fixed point so that roaming is transparent to the bridges or switches. The end devices must have IP addresses from the root IP subnet. For help, see "About Ethernet Bridging/ Data Link Tunneling" on page 134.
The end devices are unable to roam between a MobileLAN access product and 011X devices.	Set the Unicast Flood Mode to Hierarchical. For help, see "Configuring Global Flooding" on page 162.
You cannot originate an IP tunnel to an access point on a remote IP subnet.	1. Verify that the IP Router (Gateway) address is correct. 2. Verify that the access points on the ends of the tunnel have the same LAN ID. 3. On the root access point verify that the IP address of the access point at the endpoint of the IP tunnel appears in the IP Addresses list.

Table 71. General Troubleshooting (Continued)

Problem/Question	Possible Solution/Answer
You need to verify the static WEP keys.	You cannot verify the WEP keys. The keys are encrypted after you enter them and are never displayed again. You may need to reconfigure your access points and end devices to reset the WEP keys.
The filters are not filtering properly.	Check all of your filter settings. Conflicts may exist between the various filters.
You need to confirm which master radio a WAP is connected to.	To verify that a WAP is communicating with a particular radio, view the AP Connections screen for the access point. Click Maintenance > AP Connections.
The throughput seems slow.	❒ Verify that your antennas are well placed and that metal or other obstacles do not block them. ❒ You may want to add a second access point and implement roaming if you move the antenna closer to the device and throughput increases. ❒ You may be able to set filters to eliminate Ethernet traffic on the wireless network. For help, see “Configuring IP Tunnel Filters” on page 150.
The radio coverage is less than you expected it to be.	Verify that the antennas or antenna cables are plugged into the correct connectors by reading the label on the access point.

Troubleshooting the Radios

If you are having problems communicating with your wireless network, you can use the access point LEDs, error messages, Radio MAC Ping, or ICMP Echo to troubleshoot any radio problems.

Using LEDs

If the access point LEDs show the following pattern after it boots, the radio may be faulty or the configuration matrix string is incorrect. Contact your local Allied Telesyn representative to help you correct the problem.

Table 72. AT-WA7500 and AT-WA7501 LEDs

○	○	○	● or ☼ (Blinks for wired data traffic.)	● or ☼ (Blinks if the AP becomes root.)

○ LED On ● LED Off ☼ LED Flashing

Using a Communications Program or a Telnet Session

If you are communicating with the access point using a communications program or a telnet session, an error message may appear on your PC after the access point reboots or when a session is saved. The error messages are described in the following table. Contact your local Allied Telesyn representative to help you correct the problem.

In this table, “Radio A” refers to the radio in slot 1 and “Radio B” refers to the radio in slot 2. These error messages may appear for either radio.

Table 73. Radio Error Messages

Error Message	Explanation
Couldn’t read country code from radio A	The radio may be faulty.
Invalid country code in string for radio A	The country code in the configuration matrix string does not match the country code in the radio in the access point.
Radio A has unknown country code	The radio may have been configured incorrectly at the factory.
Radio string doesn’t match radio installed	When this error message appears, additional information also appears on the screen; for example, “Expected 504,000 but found 491 in slot A, nothing in slot B” may appear. The radio may be faulty.

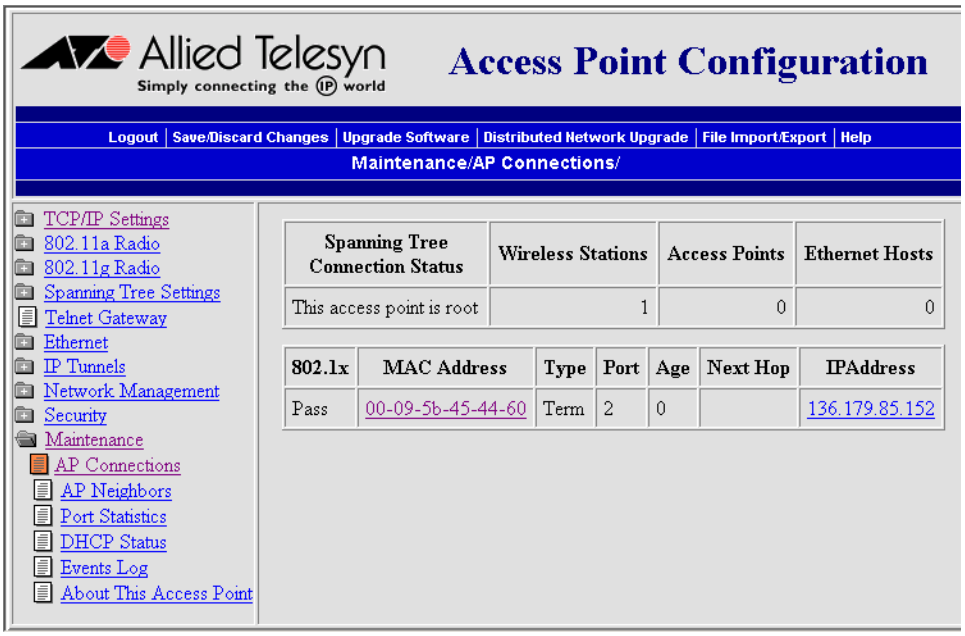
Using Radio MAC Ping (802.11g and 802.11b Radios)

Radio MAC Ping runs at the MAC sublayer of the Data Link layer, thus allowing you to ping any 802.11b device that is connected to the access point. Radio MAC Ping can help you determine the connectivity and signal strength of an 802.11b radio.

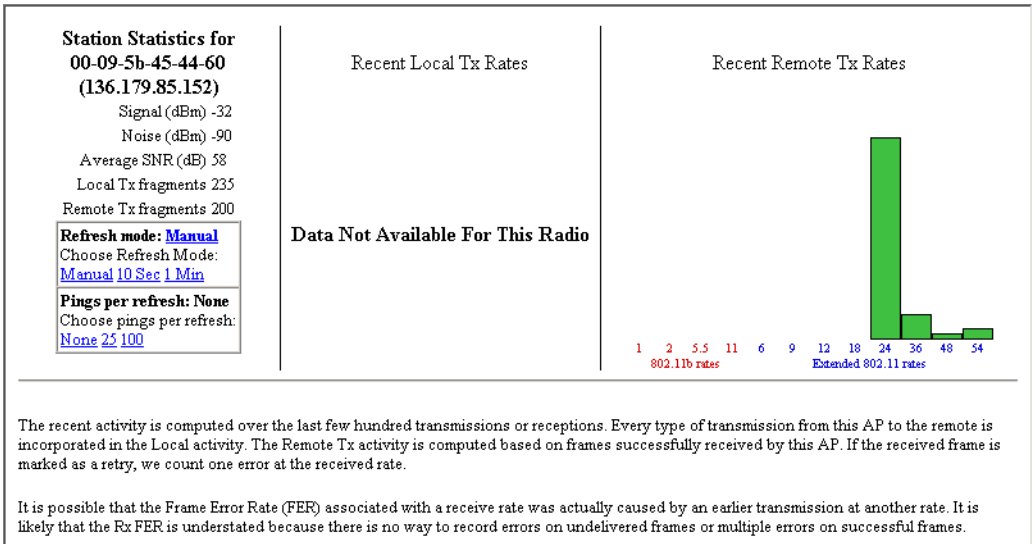
To use radio MAC ping

1. From the menu, click Maintenance > AP Connections. The AP Connections screen appears. All devices that support a radio MAC

ping will have their MAC address listed with a hyperlink.



2. Click a MAC address hyperlink. The access point pings the device, and then this screen appears showing the results.



By default, the Refresh Mode is Manual. To configure the software to refresh automatically at a set interval, click 10 Sec or 1 Min.

By default, the Pings per refresh is None. To increase the number of pings that occur after each refresh, click 25 or 100.

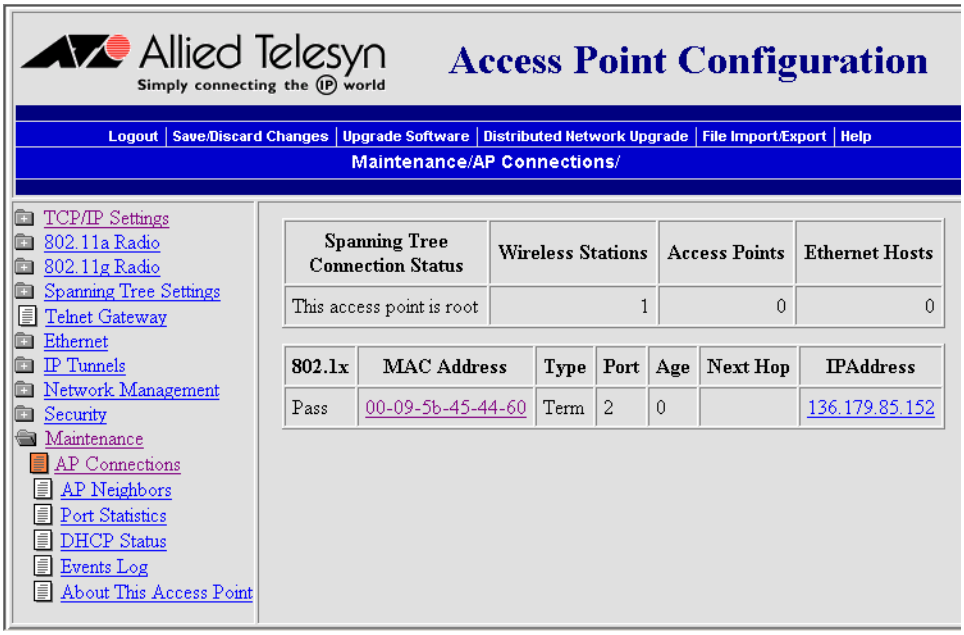
3. Click the X in the upper right corner of the window to return to the AP Connections screen.

Using ICMP Echo

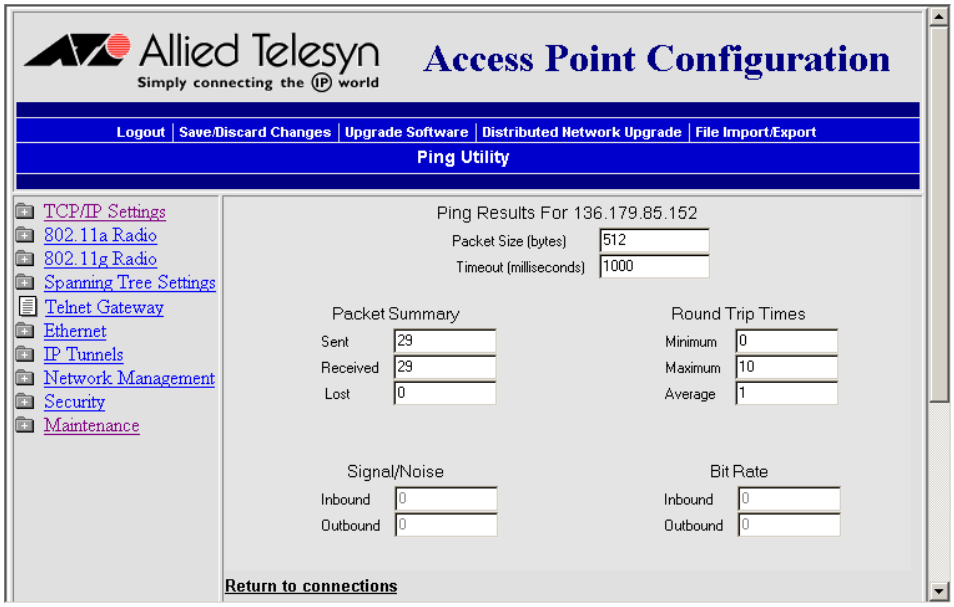
ICMP (Internet Control Message Protocol) echo lets you ping devices using their IP address. ICMP echo can only be used if the access point has determined the IP address of the end device or another access point. If the access point is acting as an ARP server, it will determine the IP addresses of the end devices that are attached to it and allow you to use ICMP echo on the wireless network. The access point always knows the IP address of all access points in the spanning tree.

To use ICMP echo

1. From the menu, click Maintenance > AP Connections. The AP Connections screen appears.



2. Click an IP address hyperlink. The access point pings the device, and then the Ping Utility screen appears showing the results.



Note
The information on this screen varies with the type of request sent and the capabilities of the medium through which it is sent. Echo requests sent through different radios may report different results.

3. Click Return to connections to return to the AP Connections screen.

Troubleshooting Security

This section helps you troubleshoot problems you may have while installing and configuring security in your network. For more help troubleshooting 802.1x security, refer to the documentation for the MobileLAN secure 802.1x security solution, the Odyssey server, and the end devices.

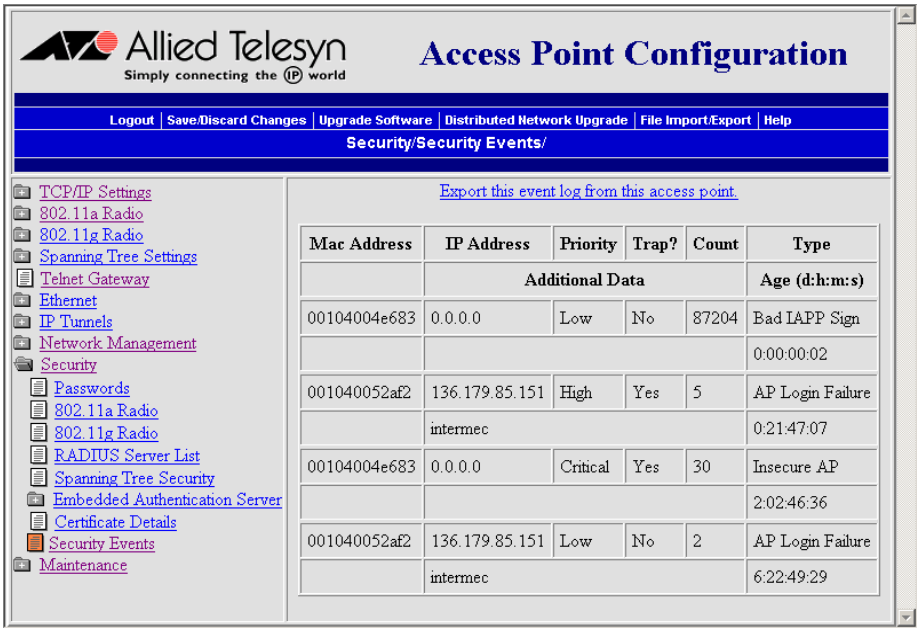
Viewing the Security Events Log

The access point logs a variety of 802.1x events in its Security Events log. Only the access point that generates the security event displays it in its Security Events log.

To see all the 802.1x events in your network, you need to use MobileLAN manager or another SNMP management station or network management tool.

To view the Security Events log

❒ From the menu, click Security > Security Events. The Security Events log appears.



For help understanding the events, see the next table.

Table 74. Security Events Log Description

Column	Description
MAC Address	Indicates the Ethernet MAC address of the device that caused the event.
IP Address	Indicates the IP address of the device that caused the event.
Priority	Indicates the priority of the event: Critical, High, Low, or Informative Critical and High priority events generate an SNMP trap.
Trap?	Specifies if the event generated an SNMP-reliable trap.
Count	Indicates the number of times the event occurred.
Type	Includes details of the event that occurred.
Additional Data	Includes extra event-specific information.
Age	Indicates the amount of time that has passed since the event occurred.

Note
If you use an SNMP management station or another network management tool, the age represents how much time has passed since the access point was booted that this event occurred.

Exporting the Security Events Log

You can export the Security Events log from the web browser interface to a comma-separated file. You can open this file using Microsoft Excel or Notepad.

To export the security events log

1. From the menu, click Security > Security Events. The Security Events log appears.
2. Click Export the Security Events Log from this access point. A File Download box may appear.
3. Click Save. The Save As dialog box appears.
4. Choose where you want to save the SECLOG.CSV file and click Save.

General Security Troubleshooting

This section provides you with information on getting help with your secure network and some problems and solutions.

Table 75. General Security Troubleshooting

Problem/Question	Possible Solution/Answer
You enabled secure IAPP in your network, but the access points do not communicate with the root access point.	❒ Verify that the root access point is running software release 1.80 or later. Upgrade all access points to the same software release as the root access point. ❒ Verify that you enabled secure IAPP on all access points. ❒ In the root access point, click Maintenance > AP Connections. If any access point station radios are blocked, re-enter the IAPP secret key in all access points.

Table 75. General Security Troubleshooting (Continued)

Problem/Question	Possible Solution/Answer
You are implementing 802.1x security and you cannot get an end device to authenticate with a RADIUS server.	❒ Verify that the root access point is running software release 1.72 or later. ❒ Verify that the RADIUS server IP address is correct. Re-enter the RADIUS server secret key in both the access point and the RADIUS server. ❒ Verify that the IAPP secret key is the same in all access points. ❒ Verify that the access point that the end device is communicating with has the 802.1x Authentication field set to authenticate the radio that is in the end device. ❒ Verify that your end device is configured properly for 802.1x security. For help, see the end device user's manual.

Recovering a Failed Access Point

Note
Do not use this procedure to upgrade your access point software. For help, see "Upgrading the Access Points" on page 261.

You should never need to use this procedure. However, if your access point is not functioning, you may need to download an entirely new file system. If the access point loses all its files except the boot ROM code, you cannot ping the access point, you cannot establish a telnet session to the access point, and the LEDs display this pattern.

Table 76. LED Pattern of a Failed Access Point

○	☼	☼	☼	●	Only Boot ROM code is available on access point. Load new files.
	(Wireless #1 and #2 blink in unison.)				

○ LED On ● LED Off ☼ LED Flashing

You can recover a failed access point using a Windows NT4/2000/XP PC. The procedure is explained in the next subsection.

Using a Windows NT4/2000/XP PC

You can use a Windows NT4/2000/XP PC and a command prompt to recover a failed access point. To access a command prompt, see your Windows documentation. For this procedure you will need to contact Allied Telesyn Technical Support to obtain the AP824X.DNL file.

To recover a failed access point

1. From a command prompt, type this command to create a static ARP cache entry for the netloader.

   `arp –s` *`x.x.x.x yy-yy-yy-yy-yy-yy`*

   where:

   *x.x.x.x*is the IP address that you want to assign the access point

*yy-yy-yy-yy-yy-yy*is the MAC address of the access point. This MAC address is printed on a label that is on the bottom of the access point.

> **Note**
> If you are only recovering one access point, you can enter 00:10:40:FF:FF:FF. This special MAC address works with all access points.

2. Type this command to continuously ping the access point while you boot the access point.

   `ping –t –l 100` *`IPaddress`*

   where *IPaddress* is the access point IP address you assigned in Step 1.

3. Disconnect and reconnect the power cable (or Ethernet cable, if you are using power over Ethernet) to the access point. The access point has no On/Off switch, so it boots as soon as you apply power.

4. When the access point responds to the ping, use any TFTP client to transfer AP824X.DNL file to the access point. Make sure the Transfer mode is binary.

   `tftp –i` *`IPaddress`* `put AP824X.dnl`

   where *IPaddress* is the access point IP address you assigned in Step 1.

Once the TFTP transfer is complete, the access point will begin booting the image that was just passed to it. This image is only resident in RAM. If you reboot the access point or if the access point loses power, the AP824X.DNL image will be lost.

5. Type this command to remove the static ARP cache entry from your PC.

   `arp –d` *`IPaddress`*

   where *IPaddress* is the access point IP address you assigned in Step 1.

   When the access point is done booting, all access point services are available. You can now telnet to the access point to upgrade it with a permanent image and configure it.

   Note
   You may be unable to access the web browser interface if the support files for this interface still need to be recovered. If so, use telnet to upgrade the access point, and then use the web browser interface to configure it.

Upgrading the Access Points

For optimal performance, you should install the most current software version on all the access points in your network. To upgrade the software, you must copy the software release to your PC and then upload the release to your root access point and other access points. However, you can also configure the root access point to copy the release to all other access points in its spanning tree.

You can upgrade the access point software using a web browser interface, as explained in the next subsection.

Note
New releases of the firmware for the access point are available for downloading from the Allied Telesyn web site.

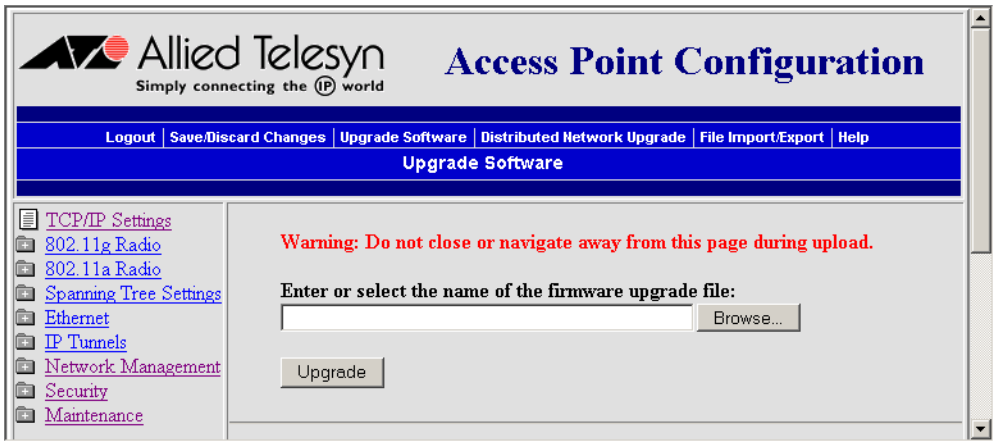
Using a Web Browser Interface

You can use a web browser interface to upgrade the access points one at a time. In other words, for each access point you want to upgrade, you will need to establish a web browser session with it, upgrade its software, save the new configuration, and reboot it.

To upgrade the access point software

1. Establish a web browser session with the access point you want to upgrade.

2. From the menu bar, click Upgrade Software. The Upgrade Software screen appears.



3. Enter the path and filename of the upgrade file (AP*WEB.BIN) or click Browse to find the file on your PC. For example, AP21WEB.BIN.

Note
If you have not already copied the upgrade file to your PC, follow the instructions in “Upgrading the Access Points” on page 261.

4. Click Upgrade to start the upgrade. The upgrade may take up to 3 minutes to complete.

5. When the upgrade is complete, click Save Changes and Reboot.

   When the access point is done rebooting, it is upgraded to the new software. Repeat this procedure for each access point you want to upgrade.

Troubleshooting the Upgrade

Each access point on a wired LAN requires approximately 3 minutes to upgrade (it takes slightly longer for wireless access points). The web browser screen updates every 30 seconds as the upgrade progresses and shows the final status when all upgrades are complete. If you checked the Reboot selected Access Points after successful upgrade check box, the web browser disconnects. Click the Refresh button to log in again.

Errors may occur during the upgrade process or during the final reboot. If an error occurs, an explanation appears on the web browser screen.

If an error occurs during the upgrade, none of the access points reboot. You should:

1. Recheck the access points where the error occurred.

2. Click Start Upgrade to attempt the upgrade again. If the upgrade is successful and you checked the Reboot selected Access Points after successful upgrade check box, the access points will reboot.

If an error occurs during the final reboot, you should:

1. Wait 5 minutes for the access points that did not reboot to refresh.

2. Refresh your web browser screen and check the access points that are not running the new version.

3. Click Start Upgrade to attempt the upgrade again. If the upgrade is successful and you checked the Reboot selected Access Points after successful upgrade check box, the access points will reboot according to your Reboot selection.

If you need to downgrade an access point to an earlier release, contact Allied Telesyn Technical Support.

Chapter 9

Additional Access Point Features

This chapter explains some of the more advanced ways that you can maintain the access points. This chapter covers these topics:

Understanding the Access Point Segments

The AT-WA7500 and AT-WA7501 access points contain one flash memory segment, as well as temporary memory (RAM).

Several of the commands described in this chapter require that you specify the segment where a file is located on the access point. To indicate the segment where the file is located, you precede the filename with either a segment number or name followed by a colon. For example, `1:ap824x.prg` refers to the AP824X.PRG file is located in segment 1.

The segment numbers (1, 2, 3, and 4) and names (id, ib, ad, and ab) actually indicate specific segments on older access points. But these numbers and names all indicate the same flash memory segment on an access point.

When you use a command that requires a segment number or name, you can specify 1, 2, 3, 4, id, ib, ad, or ab to indicate the one flash memory segment on the access point. For consistency, all the commands in this chapter use the segment number 1.

If you do not specify a segment name or number in a command, the access point first searches RAM and then the flash memory segment until it finds a file that matches the file name.

Note
Legacy scripts with commands that specify segment numbers or names can be run on AT-WA7500 and AT-WA7501 access points without generating errors.

Understanding Transparent Files

The AT-WA7500 and AT-WA7501 access points with software release 2.2 support transparent files, which are files without file headers. Transparent files all have the date May 14, 2002 (5-14-2002) and have no version.

The advantage of using file headers is that the date and file versions are correct when you use the FD command to view the directory. All provided .DNL files have file headers. All files to be uploaded by script files must have file headers.

For help using the TFTP GET command with transparent files, see page 280.

Using the AP Monitor

The AP (access point ROM) monitor is system software that lets you manipulate the access point files and file segments. You can only access the AP monitor through the serial port using a communications program.

> **Note**
> Certain functions available through the AP monitor can erase the access point configuration. Allied Telesyn strongly recommends that you only use the AP monitor when absolutely necessary. For example, you might use the AP monitor to upgrade the access point software or when instructed to do so by Allied Telesyn Technical Support.

Entering the AP Monitor

1. Use a communications program to start a session with the access point.
2. Reboot the access point.
3. When you see the message <Press any key within 5 seconds to enter the AP monitor> during the boot process, press Enter. The ap prompt (ap>) appears.

Using AP Monitor Commands

You can display a list of AP monitor commands on the screen anytime you see the ap prompt.

To list AP monitor commands

- ❒ Press any key (except the letter B, which reboots the access point), and then press Enter. A list of AP monitor commands appears.

```
AP Monitor V5.69 January 30, 2004
AP FPGA Firmware 0.14
wa21 Platform
<Press any key within 5 seconds to enter the AP monitor>
ap>d
--------------------------------------------------------------------------------
"ap>" commands...
--------------------------------------------------------------------------------
B           - Reboot                    | MR          - Display Mfg Record
FX s        - Ymodem File Download      | CAM         - CAM Menu
FD          - File System Directory     | TEST        - Test Menu
FR          - Run Flash Startup File    | SRVC        - Service Menu
            - Manufacturing Menu        | SR z        - Serial Baud Rate
            - Device IDs Menu           |
--------------------------------------------------------------------------------
ap>
```

B

Purpose: Reboots the access point.

Syntax: B

FD

Purpose: Displays the flash file system directory, including information about the boot file.

Syntax: FD

FR

Purpose: Finds the first executable file in the access point boot segment and tries to run it; therefore, the first executable file in the access point boot segment must be the boot file.

Syntax: FR

FX

Purpose: Downloads a file using Ymodem batch protocol into the flash segment that is specified by s.

Syntax: FX *s*

where s is destination segment. You can use any number (1, 2, 3, or 4) to specify the one flash memory segment on the access point.

MR

Purpose: Displays the manufacturing record for the access point. Use the MR command to display the MAC address, configuration string, and serial number for your access point.

Syntax: MR

SR

Purpose: Sets the baud rate of the access point.

Syntax: SR *z*

where z is the baud rate. You must enter the baud rate as a whole number with no commas. For example, to enter a baud rate of 19,200, you must enter 19200.

You can also set the baud rate to autobaud, which lets the access point set its baud rate to match the baud rate of your wireless end device. Type SR 0 and press Enter twice.

Using Content Addressable Memory (CAM) Mode Commands

You may need to use CAM commands to perform certain functions. Since the Ethernet port on the access points supports data rates significantly higher than the radio ports, all frames cannot be forwarded from the Ethernet network to the radios. CAM, which is controlled by the Field Programmable Gate Array (FPGA), filters frames based on the radio's capability.

Because the commands can cause undesirable results if not properly executed, you should contact Technical Support for assistance if you are unsure about the proper procedure to use.

To enter CAM mode

1. Type CAM and press Enter.
2. Enter a password. The default password is EV98203C (case sensitive).

When you are in CAM mode, the CAM prompt (CAM>) appears.

To exit CAM mode

❒ At the CAM prompt, type X and press Enter.

You return to the ap prompt.

To display CAM commands

- Type any letter or number other than B and press Enter. The CAM commands appear on the screen.

```
ap>
ap>
ap>
ap>
ap>
ap>
ap>
ap>
ap>
ap>cam
Enter password : ********
CAM>d
-------------------------------------------------------------------------------
"CAM>" commands...
-------------------------------------------------------------------------------
ADD A {T}    - Add Entry                | STS         - Show Status register
DEL A        - Delete Entry             | CON         - Show Config register
FND A        - Find Entry               | TST         - Tests CAM/FPGA
CMD R C      - Execute CAM command      | X           - Exit
REG R        - Show Register Value      |
-------------------------------------------------------------------------------
CAM>x
P
ap>
```

Using Test Mode Commands

Within the AP monitor, Test mode lets you perform certain test functions.

Because the commands can cause undesirable results if not properly executed, you should contact Technical Support for assistance if you are unsure about the proper procedure to use.

To enter Test mode

1. Type TEST and press Enter.
2. Enter a password. The default password is EV98203T (case sensitive).

When you are in Test mode, the test prompt (test>) appears.

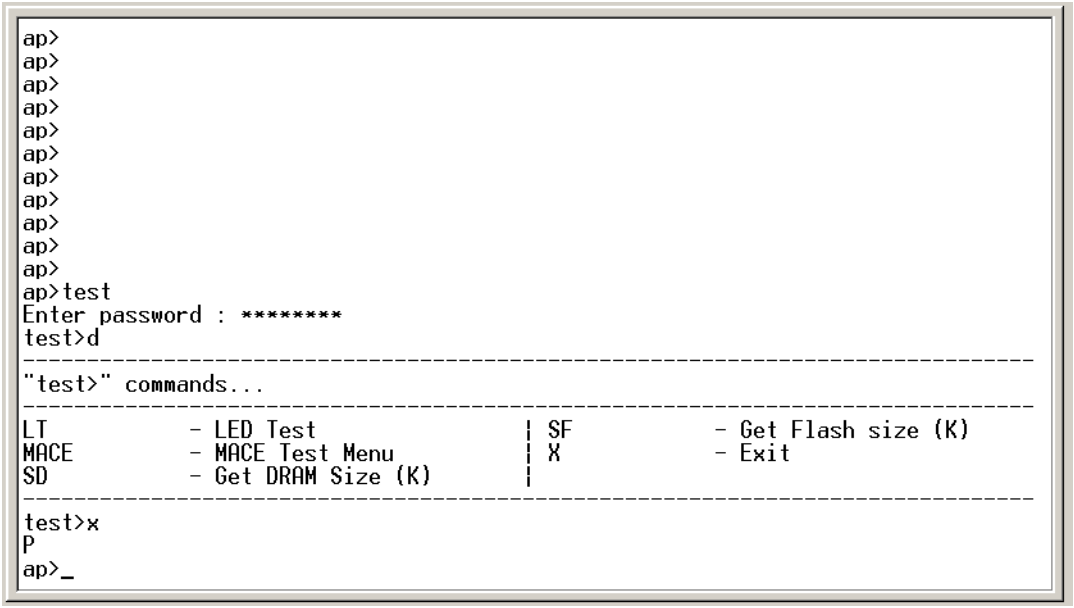
To exit Test mode

- At the test prompt, type X and press Enter.

You return the ap prompt.

To display test commands

- ❒ Type any letter or number other than B and press Enter. The test commands appear on the screen.



Using Service Mode Commands

In Service mode, you can perform file functions and segment functions such as deleting a file, downloading a file using the Ymodem protocol, and erasing a segment.

To enter Service mode

1. At the ap prompt, type SRVC and press Enter.
2. Enter the service password. The default password is EV98203S (case sensitive).

   The service prompt (service>) appears.

To exit Service mode

- ❒ At the service prompt, type X and press Enter.

You return the ap prompt.

To list service commands

- ❒ Press any key (except the letter B, which reboots the access point), and then press Enter. The service commands appear on the screen.

```
ap>
ap>
ap>
ap>
ap>
ap>
ap>
ap>
ap>srvc
Enter password : ********
service>d
-------------------------------------------------------------------------------
"service>" commands...
-------------------------------------------------------------------------------
FD          - File System Directory    | FX s        - Ymodem File Download
FDEL f {s}  - File Delete              | EC          - Erase configuration
FC <s|all>  - Compact Segment(s)       | HDW f {s}   - save FPGA config file
FE <s|all>  - Erase Segment(s)         | FB bs {ds}  - Set Boot/Data Segments
FI {s}      - File System Reset        | B           - Reboot
FFR f {s}   - Run File                 | X           - Exit
-------------------------------------------------------------------------------
service>x
P
ap>_
```

Many of the commands that are available in Service mode are also available in the AP monitor or Console Command mode.

B

Purpose: Reboots the access point.

Syntax: B

FB

Purpose: Makes an inactive segment the active segment. Because the access point has only one flash memory segment, this command has no affect on an AT-WA7500 or AT-WA7501. This command is included here for backward compatibility with older scripts only.

Syntax: FB *bootsegment* (*datasegment*)

where:

bootsegment is the name or number of the boot segment to be activated.

datasegment is the optional name or number of the data segment to be activated.

Example: These examples apply to non-AT-WA7500 and AT-WA7501products and are included for your reference only.

To make segment 2 the active boot segment and segment 4 the active data segment, enter:

```
FB 2 4
```

You can use an asterisk instead of a segment name if you want to leave that segment unchanged. For example, to leave the active boot segment unchanged and make segment 4 the active data segment, you could enter:

```
FB * 4
```

After loading software into the access point a common task is to activate the new software. To activate the new software, enter:

```
FB IB: ID:
```

This command activates the inactive boot and data segments. You do not need to know which of the boot and data segment numbers the flash is loaded into.

FC

Purpose: Compacts the files in a particular segment.

Syntax: FC *s*

where s indicates the segment to be compacted. You can use any segment number or name to specify the one flash memory segment on the access point.

Example: To compact the contents of the flash memory segment, enter:

```
FC 1
```

FD

Purpose: Displays the flash file system directory, including information about the boot file and the file type: E (executable), D (data), and T (transparent). For information about transparent files, see “Understanding Transparent Files” on page 265.

Syntax: FD

Example: To display the contents of the flash memory segment, enter:

```
FD
```

To display the contents of the memory card, enter:

```
FD APP:
```

FDEL

Purpose: Deletes a particular file.

> **Note**
> When you use the FDEL command, the file is marked as invalid and remains in the file system. To reclaim the file space, you must erase the entire segment. Use the FE command to erase a segment.

Syntax: FDEL *f* (*s*)

where:

f is the name of the file to be deleted.

s is the optional segment location of the file.

Examples: To delete the file AP824X.PRG from the flash memory segment, enter:

```
FDEL 1:AP824X.PRG
```

To delete the file FILE.DAT from the optional memory card on an AT-WA7500, enter:

```
FDEL APP:FILE.DAT
```

FE

Purpose: Erases all the files in a particular segment, including those that have been "deleted" with FDEL. To recover the files after they have been erased, you must reload them from another source.

> **Note**
> You must execute this command before you execute a TFTP transfer.

Syntax: FE *s*

where s indicates segment to be erased. You can use any segment number or name (1, 2, 3, 4, id, ib, ad, or ab) to specify the one flash memory segment on the access point.

Example: To erase the contents of the flash memory segment, enter:

```
FE 1
```

To erase the contents of the memory card, enter:

```
FE APP:
```

FFR

Purpose: Runs a program f, from a location s.

Syntax: FFR *f* (*s*)

where:

f is the program name.

s is the optional segment location of the program.

Example: To run program UAPBOOT.PRG from the flash memory segment, enter:

```
FFR UAPBOOT.PRG 1
```

FI

Purpose: Reinitializes the access point file system. If the access point file system or a file segment becomes corrupt, use this command to reset it.

Syntax: FI (*s*)

where s is the optional number of the segment to be reinitialized. You can use any segment number (1, 2, 3, or 4) to specify the one flash memory segment on the access point.

FX

Purpose: Downloads a file using Ymodem batch protocol into the flash segment that is specified by s.

Syntax: FX *s*

where s is destination segment. You can use any segment number (1, 2, 3, or 4) to specify the one flash memory segment on the access point.

HDW

Purpose: Loads the FPGA configuration file into the access point. If you are directed to change the FPGA firmware in the access point, use this command.

Syntax: HDW *f* (*s*)

where:

f is the FPGA configuration filename.

s is the optional segment where you want to load the configuration file.

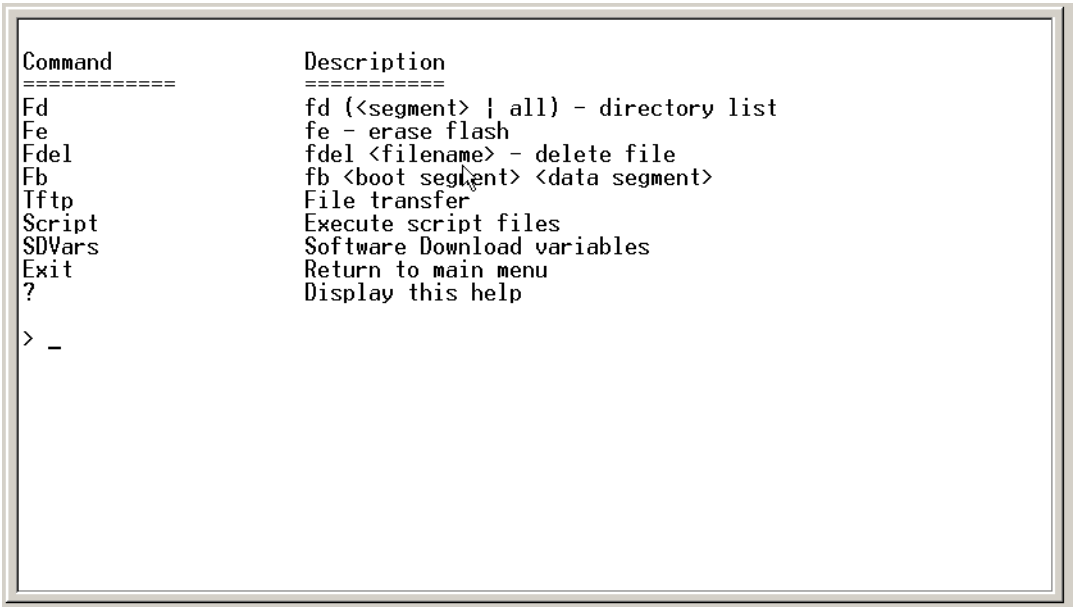
Using Command Console Mode

You can use the Command Console mode to manipulate some access point files and file segments. You can also use Command Console mode to upgrade access points using TFTP and script files.

You access the Command Console mode through the serial port using a communications program or over the network using a telnet session. You cannot access Command Console mode using a web browser interface.

Entering Command Console Mode

1. Use a communications program or telnet to start a session with the access point. For help, see “Using a Communications Program” on page 40.
2. From the Access Point Configuration menu, choose Maintenance.
3. From the Maintenance menu, choose Command Console. The list of commands appears.


Command Description
Fd fd (| all) - directory list
Fe fe - erase flash
Fdel fdel <filename> - delete file
Fb fb <boot segment> <data segment>
Tftp File transfer
Script Execute script files
SDVars Software Download variables
Exit Return to main menu
? Display this help
>

To exit Command Console mode

- At the prompt, type exit.

You return to the Maintenance menu.

Using the Commands

Several of these commands require that you enter filenames. To indicate the segment where the file is located, you precede the filename with either a segment number or name followed by a colon. For example, `1:ap824x.prg` refers to the AP824X.PRG file is located in segment 1.

For details about using segment numbers and names for an access point, which contains only one flash memory segment, see "Understanding the Access Point Segments" on page 264.

FB

Purpose: Makes an inactive segment the active segment. Because the AT-WA7500 and AT-WA7501 have only one flash memory segment, this command has no affect on the access points. This command is included here for backward compatibility with older scripts only.

Syntax: FB *bootsegment datasegment*

where:

bootsegment is the name or number of the boot segment to be activated.

datasegment is the name or number of the data segment to be activated.

Example: These examples apply to non-AT-WA7500 and AT-WA7501 products and are included for your reference only.

To make segment 2 the active boot segment and segment 4 the active data segment, enter:

```
FB 2 4
```

You can use an asterisk instead of a segment name if you want to leave that segment unchanged. For example, to leave the active boot segment unchanged and make segment 4 the active data segment, you could enter:

```
FB * 4
```

After loading software into the access point a common task is to activate the new software. To activate the new software, enter:

```
FB IB: ID:
```

This command activates the inactive boot and data segments. You do not need to know which of the boot and data segment numbers the flash is loaded into.

FD

Purpose: Displays the flash file system directory, which includes information about the boot file and file type: E (executable), D (data), and T (transparent). Use this command to ensure that the correct version of the file is in the active boot segment. For information about transparent files, see “Understanding Transparent Files” on page 265.

Syntax: FD

Example: To display the files loaded in the flash memory segment, enter:

```
FD 1
```

Note
If the flash memory segment contains no files when you reboot the access point, the access point enters the AP monitor and you will no longer be able to telnet to it during this session. If this occurs, you must access the access point through its serial port to correct the problem.

To show the files loaded in the memory card, enter:

```
FD app:
```

FDEL

Purpose: Deletes a particular file.

Note
When you use the FDEL command, the file is marked as invalid and remains in the file system. To reclaim the file space, you must erase the entire segment. Use the FE command to erase a segment.

Syntax: FDEL *f*

where f is the name of the file to be deleted.

Example: To delete the file AP824X.PRG from the flash memory segment, enter:

```
FDEL 1:AP824X.PRG
```

To delete the file FILE.DAT from the memory card, enter:

```
FDEL APP:FILE.DAT
```

FE

Purpose: Erases all the files in a particular segment, including those that have been "deleted" with FDEL. To recover the files after they have been erased, you must reload them from another source.

> **Note**
> You must execute the FE command before you execute a TFTP transfer.

Syntax: FE *s*

where s is the segment to be erased. You can use any segment number or name (1, 2, 3, 4, id, ib, ad, or ab) to specify the one flash memory segment on the access point.

Example: To erase the contents of the flash memory segment, enter:

```
FE 1
```

To erase the contents of the memory card, enter:

```
FE app:
```

SCRIPT

Purpose: Executes a specified file as a list of console commands. You can create a script file to automate a software download.

Syntax: SCRIPT *f*

where f is the name of the script file to be executed.

For more information about using the script command, see "Creating Script Files" on page 288.

Using TFTP Commands

TFTP commands are file transfer commands. An access point can act as either a client or server in the TFTP environment. As a server, the access point can service read and write requests from an access point client. As a client, the access point can read files from and write files to any TFTP server on the network. Both the client and server must operate in octet, or 8-bit, mode.

When executing a script file, the access point retries TFTP client commands get and put until the command is successfully completed. If the first attempt fails, the access point retries after a one-minute delay. With each successive failure, the retry time doubles until it reaches eight minutes. Once this limit is reached, it remains at eight minutes until the command is completed.

In general, TFTP client sessions should fail only if the server is not responding either because it is busy serving other clients or because it has not been started. In either case, the access point backoff algorithm should prevent excessive network traffic when many access points are trying to contact a TFTP server.

TFTP GET

Purpose: TFTP client requests a file from the TFTP server.

> **Note**
> You must use the FE command to erase the segment before you execute a TFTP GET command. If you do not erase the segment, you may get a “can’t write file” error.

Syntax: TFTP GET *IPaddress foreignfilename localfilename*

where:

IPaddress is the IP address or DNS name of the server. You can use an asterisk (*) here if you want to use the value in the internal variable serveripaddress (as defined on page 284).

foreignfilename is the name of the file on the server. The filename can contain directory path information and must be in the format required by the server operating system. The file must already have the appropriate file header before the transfer to the access point.

localfilename is the name you wish to call the file on the access point. The name must begin with a segment number or name followed by a colon. You may or may not have to specify a filename after the colon: if the file has a header, the filename is optional; if the file does not have a header, the filename is required.

Example: If the file has a header, you do not have to include a filename as part of the localfilename because the filename is set to the filename embedded in the file header on the server:

```
TFTP GET * file.dat 1:
```

If the file is a transparent file (without a header), you must include a filename as part of the localfilename:

```
TFTP GET * file.dat 1:file.dat
```

The following command gets file UAP.DNL from a directory on a PC server with IP address 1.2.3.4 and stores it in the flash memory segment on the access point.

```
TFTP GET 1.2.3.4 C:\STARTUP\UAP.DNL 1:
```

The access point may generate these error messages when it issues a TFTP GET command. Other error messages may be returned from the server and displayed by the access point. See your server documentation for additional information.

Table 77.

Error Message	Explanation
Can't write file	The file may be too big. The file may not have an access point file header (filehdr.exe). The file name may be incorrectly formed. The file may already exist in the segment and cannot be overwritten. You must erase the file first.
Invalid opcode during read	This error should not occur under normal operating conditions. This error indicates a TFTP protocol error that will not occur when you use TFTP servers that conform to the protocol.

TFTP PUT

Purpose: Copies a file from a TFTP client to the TFTP server or to another access point.

Syntax: TFTP PUT *IPaddress foreignfilename localfilename*

where:

IPaddress is the IP address or DNS name of the server. You can use an asterisk (*) here if you want to use the value in the internal variable serveripaddress (as defined on page 284).

foreignfilename is the name of the file as it will appear on the server. The file name can contain directory path information and must be in the format required by the server operating system.

localfilename is the name of the file to be sent from the access point.

Example: The following command takes file AP824X.PRG that is saved in the active boot drive on the access point client and stores it in the flash memory segment on the access point server that has IP address 1.2.3.4.

```
TFTP PUT 1.2.3.4 IB:AP824X.PRG 1:AP824X.PRG
```

The access point may generate these error messages when it issues a TFTP PUT command. Other error messages may be returned from the server and displayed by the access point. See your server documentation for additional information.

Table 78.

Error Message	Explanation
Can’t read file	The requested file may not exist.
Invalid opcode during put	This error should not occur under normal operating conditions. This error indicates a TFTP protocol error that will not occur when you use TFTP servers that conform to the protocol.

TFTP SERVER LOG

Purpose: The access point can function as a TFTP server. You can use the TFTP server log command to save a history of TFTP client requests. The TFTP server log contains useful TFTP server status information. The log begins when you set up the server. To clear the log, reboot the access point.

Syntax: TFTP SERVER LOG

TFTP SERVER START

Purpose: Use this command to enable the access point to act as a server. You can enable one access point to act as a TFTP server and download files to additional access points.

Syntax: TFTP SERVER START *access*

where access is blank for read-only access (default), or rw for read/write access. TFTP does not require any authentication, so a read/write TFTP server is very insecure and should be used only briefly. When the access point boots, read-only access is restored.

After you issue this command, the access point responds to TFTP client requests that are directed to its IP address. When acting as a server, the access point supports up to four concurrent TFTP sessions.

TFTP SERVER STOP

Purpose: When you are done transferring files, you can stop the access point from being a TFTP server by using this command.

Syntax: TFTP SERVER STOP

After you issue this command, the access point no longer responds to TFTP client requests; however, current TFTP sessions with the server are allowed to complete. This table lists error messages that can be issued from the TFTP server. These messages are sent to the client and should be read from the client perspective.

Table 79. TFTP Server Stop

Error Message	Explanation
TFTP server only supports octet mode	The client is attempting to transfer a file in ASCII mode. The access point TFTP server only supports octet mode, which includes binary and image.
Unable to open remote file	The TFTP server cannot open the file that is named in the read or write request. If you are trying to read a file, the file may not exist. If you are trying to write a file, the file may be too big, the file may not have an access point file header, or the file name may be incorrectly formed.
Can't read remote file	The server returns this message if the access point file system returns an error while the server is attempting to read the file. This message is unlikely to occur.
Can't write remote file	The server returns this message if the access point file system returns an error while the server is attempting to write the file. This message is unlikely to occur.
TFTP opcode not read or write request	This error should not occur under normal operating conditions. This error indicates that the TFTP client does not conform to the protocol.
Invalid opcode during read	This error should not occur under normal operating conditions. This error indicates that the TFTP client does not conform to the protocol.

Table 79. TFTP Server Stop

Error Message	Explanation
Invalid opcode during write	This error should not occur under normal operating conditions. This error indicates that the TFTP client does not conform to the protocol.

Using sdvars Commands

Use sdvars commands to manipulate certain software download variables. Sdvars commands support both GET and SET arguments. You can enter sdvars commands to GET a software download object, and then issue the sdvars command using the SET argument to assign the object a specified value.

This section describes the sdvars commands using the SET argument. To execute an sdvars command using the GET argument, omit the variable from the end of the command.

sdvars set serveripaddress

Purpose: Sets the internal variable called serveripaddress to a specified address.

Syntax: sdvars set serveripaddress *ipaddress*

where ipaddress is the address of the TFTP server.

Example: To set the IP address of the server to 192.168.49.29, enter:

sdvars set serveripaddress 192.168.49.29

sdvars set scriptfilename

Purpose: Sets the internal variable scriptfilename to a specified string. The specified string should be the filename of the script to be retrieved from the TFTP server.

Syntax: sdvars set scriptfilename *foreignfilename*

where foreignfilename is a script filename on the TFTP server.

Example: To set the scriptfilename to SCRIPT.DAT, enter:

```
sdvars set scriptfilename script.dat
```

sdvars set starttime

Purpose: Sets the internal variable starttime. Starttime is a countdown time; that is, when zero is reached, the software download process begins. Set this variable to reflect how far into the future the access point is to begin downloading and executing the script file from the TFTP server. When the timer reaches 0, the access point uses the values in serveripaddress and scriptfilename to get the script file that is to be executed. If either serveripaddress or scriptfilename contains no value, an error is noted in the status variable and the software download process is terminated.

Syntax: sdvars set starttime *dd*:*hh*:*mm*:*ss*

where dd:hh:mm:ss is how far in the future the reboot is to begin and

dd is days.

hh is hours.

mm is minutes.

ss is seconds.

Example: To begin the script file download in 5 minutes, enter:

```
sdvars set starttime 00:00:05:00
```

> **Note**
> If you need to stop the download, you can do so by setting starttime to 0 if it has not already been reached by the countdown. Resetting starttime to 0 stops the timer and the download process.

sdvars set checkpoint

Purpose: Sets the internal variable called checkpoint to a specified value. The checkpoint variable is useful for monitoring the progress of a script file as it is executed. You can set the checkpoint variable to a different value after each script command, and then query the checkpoint value using SNMP to determine the progress of the download.

Syntax: sdvars set checkpoint *value*

where value is a whole number.

Example: Consider the following script file commands:

```
sdvars set checkpoint 1

fe 1
```

```
sdvars set checkpoint 2

TFTP get * ap824x.prg 1

sdvars set checkpoint 3

reboot
```

When the software download is started, you can use SNMP to query its progress by reading the checkpoint variable. If the variable has a value of 2, you know that the access point is trying to execute the TFTP get statement. If the value is 3, you know the script has completed and the reboot was executed. The value of the checkpoint variable may also be helpful in determining where an error occurred if the script fails.

sdvars set terminate

Purpose: Sets the internal variable terminate to a specified value. Use terminate to stop a countdown process in the access point. If either starttime or nextpoweruptime is counting down, setting this variable stops the timer and halts the countdown process.

> **Note**
> You should use caution when using this command. If the script file is being downloaded or executed, setting this variable interrupts the processing and can leave the access point in an undetermined state that may require user intervention.

Syntax: sdvars set terminate

sdvars set setactivepointers

Purpose: Sets the setactivepointers command to change inactive segments to active segments the next time the access point is rebooted. This command is usually used with the nextpoweruptime command.

Syntax: sdvars set setactivepointers none/boot/data/both

where:

none does not change the active segments. The default is none. Also, when the reboot is completed, the access point resets this value to none.

boot changes the inactive boot segment to the active boot segment.

data changes the inactive data segment to the active data segment.

both changes both the boot and data inactive segments to the active segments.

Example: To change the inactive boot and data segments to active at the next reboot, enter:

```
sdvars set setactivepointers both
```

sdvars set nextpoweruptime

Purpose: Sets the nextpoweruptime command to set the internal variable nextpoweruptime to a countdown time so that when 0 is reached, the access point will reboot. When the nextpoweruptime counter reaches 0, the access point checks the value of the setactivepointers variable, takes the appropriate action, and then reboots.

> **Note**
> If you need to terminate the reboot, you can set nextpoweruptime to 0 if it has not already been reached by the countdown. By resetting nextpoweruptime to 0, the timer stops so the access point does not reboot.

Syntax: sdvars set nextpoweruptime *dd*:*hh*:*mm*:*ss*

where dd:hh:mm:ss is how far in the future the reboot is to begin and

dd is days.

hh is hours.

mm is minutes.

ss is seconds.

Example:

To reboot the access point 2 hours from now, enter:

```
sdvars set nextpoweruptime 00:02:00:00
```

Creating Script Files

You can create a script file that executes a series of commands. For example, when you upgrade the access point, you typically need to erase the flash memory segment, download the new files, and reboot using the new software. You can create a script file to perform these commands.

Script files are ASCII text files with a 32-byte file system header appended. You may need to contact your local representative for a copy of the header file called FILEHDR.EXE. Follow these rules when creating script files:

- The total file size including the header must be less than 4096 bytes, which is the size of the RAM file segment.
- Each line in the script file must have fewer than 80 characters
- Each line in the script file must be terminated by an LF or CR.
- You can only have one command per line.
- Any file that is to be uploaded by script must have a file header. This does not include the script file itself.
- You can include comments on a line by using the pound (#) sign; all characters after a pound sign are ignored.

To test a script file, log onto an access point and type each of the script file commands.

New Sample Script for Upgrading an Access Point

This new sample script upgrades an AT-WA7500 or AT-WA7501 access point. This script is based on upnopath.dnl, which is included in the AP upgrade package. A header file is not required. All files are copied into segment 1: on the access point.

Sample script file for upgrading an access point

```
file sdvars set checkpoint 1

file fe 1:

file sdvars set checkpoint 2

file tftp get * software\ap824x.dnl 1:

file tftp get * software\boot824x.dnl 1:

file tftp get * software\act.dnl 1:

file tftp get * software\ap3890.dnl 1:

file tftp get * software\applets.dnl 1:
```

```
file tftp get * software\cert.dnl 1:
file tftp get * software\closed.dnl 1:
file tftp get * software\discinca.dnl 1:
file tftp get * software\easdb.dnl 1:
file tftp get * software\echo.dnl 1:
file tftp get * software\favicon.dnl 1:
file tftp get * software\file.dnl 1:
file tftp get * software\fileimp.dnl 1:
file tftp get * software\filemenu.dnl 1:
file tftp get * software\fpga8245.dnl 1:
file tftp get * software\fsys.dnl 1:
file tftp get * software\help.dnl 1:
file tftp get * software\hlp.dnl 1:
file tftp get * software\jsutil.dnl 1:
file tftp get * software\login.dnl 1:
file tftp get * software\logo.dnl 1:
file tftp get * software\logo2.dnl 1:
file tftp get * software\menu.dnl 1:
file tftp get * software\netdwnl.dnl 1:
file tftp get * software\open.dnl 1:
file tftp get * software\sftdwnl.dnl 1:
file tftp get * software\sta3890.dnl 1:
file tftp get * software\stastats.dnl 1:
file tftp get * software\tbldata.dnl 1:
file tftp get * software\tftpcl.dnl 1:
file tftp get * software\tftpsrv.dnl 1:
file tftp get * software\welcome.dnl 1:
file sdvars set checkpoint 5
file sdvars set NextPowerUpTime 00:00:00:5
```

Legacy Sample Script for Upgrading Any Access Point

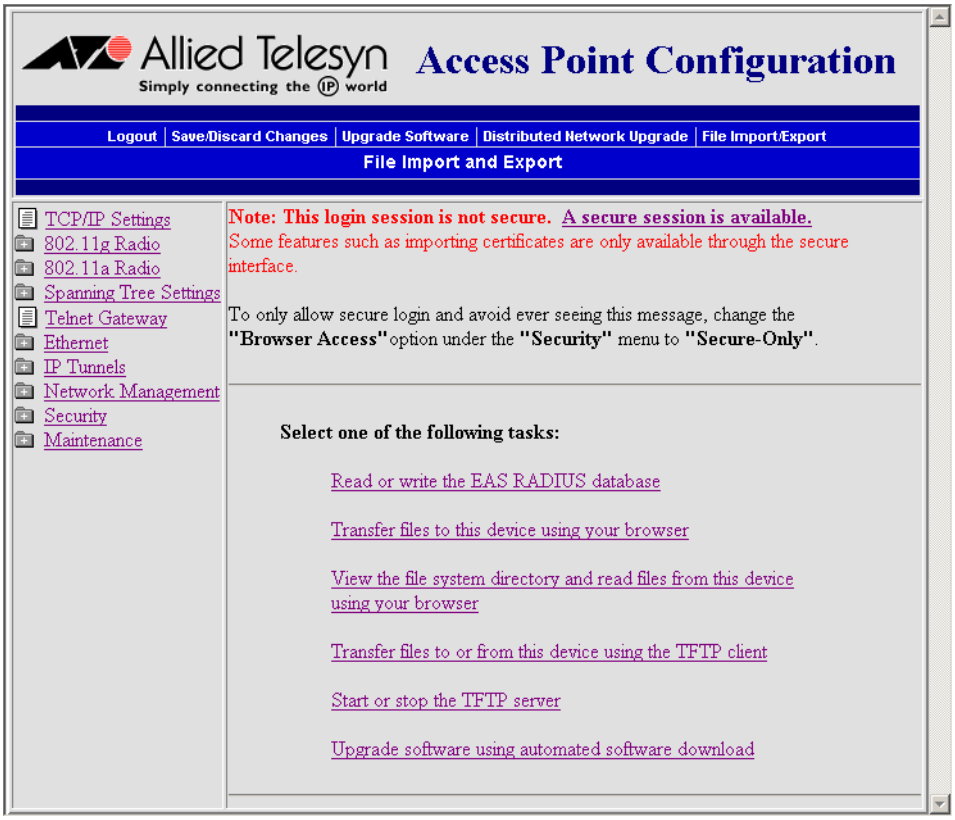
This sample script file was created for older access points with multiple segments. Although this script specifies segments that do not exist on AT-WA7500 and AT-WA7501 access points, you can run this script on the access points without generating errors.

For help understanding these commands, see the command descriptions in this chapter.

```
#Sample script file for upgrading an access point

#Step 1: Delete files

file sdvars set checkpoint 1

file fe ib:

file fe id:

#Step 2: Get boot files

file sdvars set checkpoint 2

file tftp get * \data\bootchk.dnl ib:

file tftp get * \startup\uap.dnl ib:

file tftp get * \startup\uapboot.dnl ib:

#Step 3: Get data files

file sdvars set checkpoint 3

file tftp get * \data\bkgrnd.dnl id:

file tftp get * \data\bootchk.dnl id:

file tftp get * \data\discinca.dnl id:

file tftp get * \data\falcon_.dnl id:

file tftp get * \data\help.dnl id:

file tftp get * \data\hlp.dnl id:

file tftp get * \data\intermec.dnl id:

file tftp get * \data\menu.dnl id:

file tftp get * \data\sftdwnl.dnl id:

file tftp get * \data\welcome.dnl id:

file tftp get * \data\write.dnl id:

#Step 4: Set checkpoint to show completed

file sdvars set checkpoint 4
```

Copying Files To and From the Access Point

You can accomplish a variety of file import/export tasks from the File Import/Export screen. In the menu bar, click File Import/Export, and the File Import and Export screen appears.



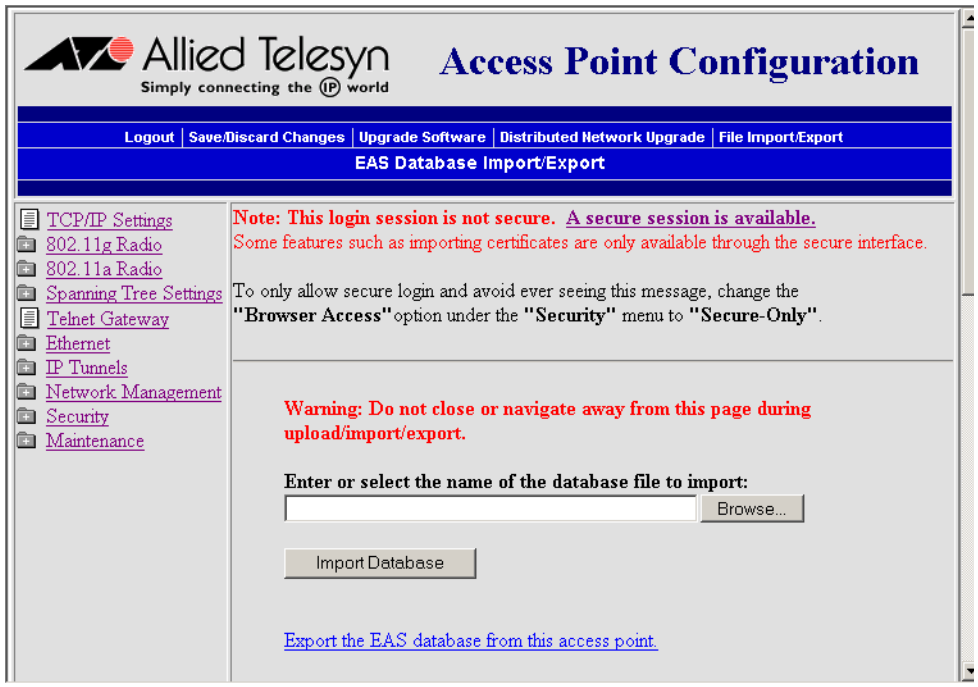
From this screen you can perform these tasks, which are described next:

- To import or export an EAS RADIUS database file
- To transfer files to the access point using your web browser
- To view and copy files from the access point using your web browser
- To transfer files to and from a TFTP server
- To start or stop the TFTP server
- To automatically upgrade software (in a network with older access point software)

Importing or Exporting an EAS RADIUS Database File

To import or export an EAS RADIUS database file

1. Click Read or write the EAS RADIUS database. The EAS Database Import/Export screen appears.



2. To import a file, enter of select the name of the database file to import and click Import Database.

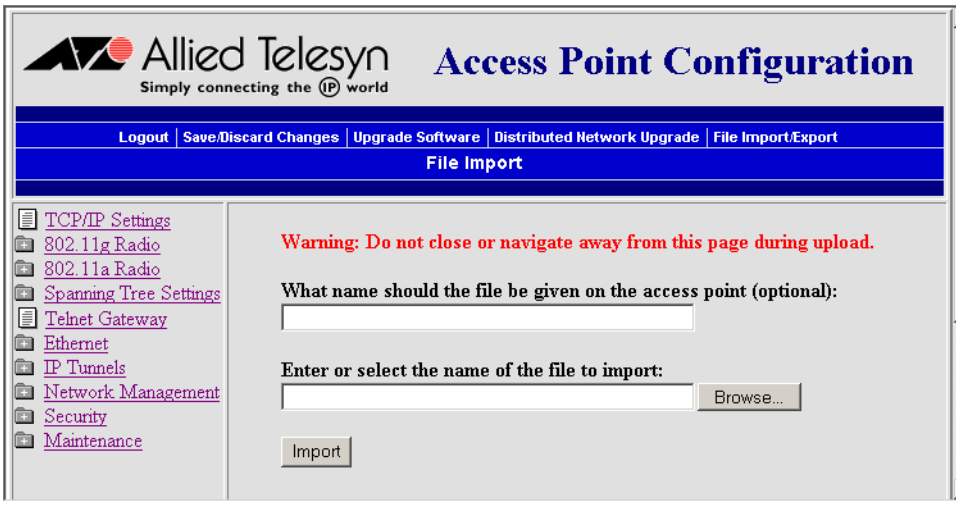
> **Note**
> For details about the purpose and format of import files, scroll down this screen and read the help text.

3. To export a database, click Export the EAS database from this access point. The export link can be used to extract the current database from the access point into a comma separated text file format. This file can be used to propagate the database to another access point. 802.1x (PEAP) entries are exported as type 802.1x (TTLS) entries.

Transferring Files Using Your Web Browser

To transfer files to the access point using your web browser

1. Click Transfer files to this device using your browser. The File Import screen appears.



2. (Optional) You can type a filename in the first input field to specify the name that the file will have on the access point.

   To import a file to the memory card, use the app segment identifier alone (app) or with a file name (app:test.txt).

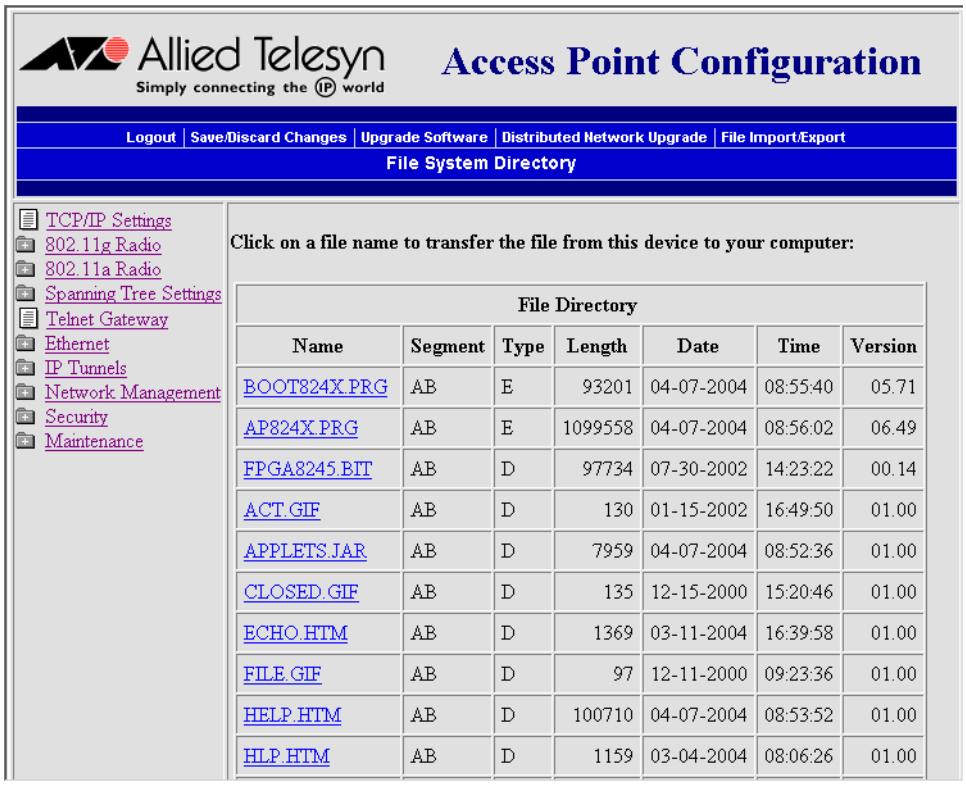
3. In the second input field, type the file name or click Browse to select the file to be imported to the device.

4. When the correct file name is displayed in the input field, click Import to start the file transfer.

Viewing and Copying Files Using Your Web Browser

To view and copy files from the access point using your web browser

1. Click View the file system directory from this device using your browser. The File System Directory screen appears.



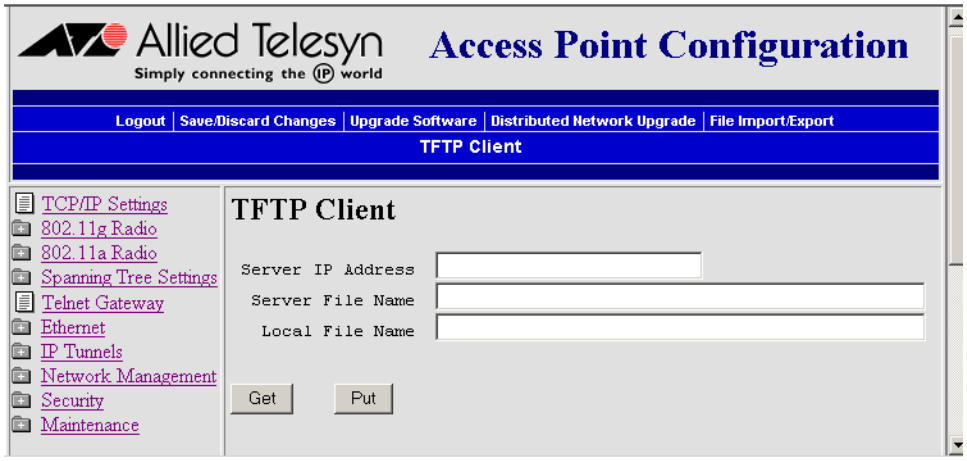
Note
The segment column on this screen contains the identifier AB, which indicates that single flash memory segment on an access point. For help, see “Understanding the Access Point Segments” on page 264. The segment column could contain APP, which would indicate a file stored on the memory card.

2. Click any file name to transfer the file from the access point to your PC.

Transferring Files to and from a TFTP Server

To transfer files to and from a TFTP server

1. Click Transfer files to or from this device using the TFTP client. The TFTP Client screen appears.



2. In the Server IP Address field, enter the IP address or DNS name of the TFTP server.

3. In the Server File Name field, type the name in the format required by the operating system of the server.

4. In the Local File Name field, type the file name for the file on the device. Access point filenames (for software release 2.2 or later) use this format: segment:filename, where segment is 1 for memory or app for the memory card.

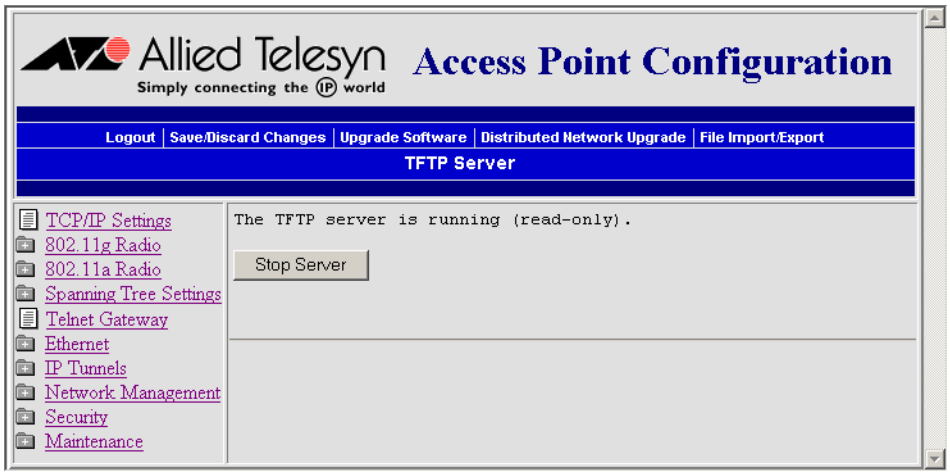
   When performing TFTP GET commands, this field need only contain the segment identifier (1 or app) because the file name is determined by the header of the downloaded file.

5. Click Get or Put.

Starting or Stopping the TFTP Server

To start or stop the TFTP server

1. Click Start or stop the TFTP server. The TFTP Server screen appears.



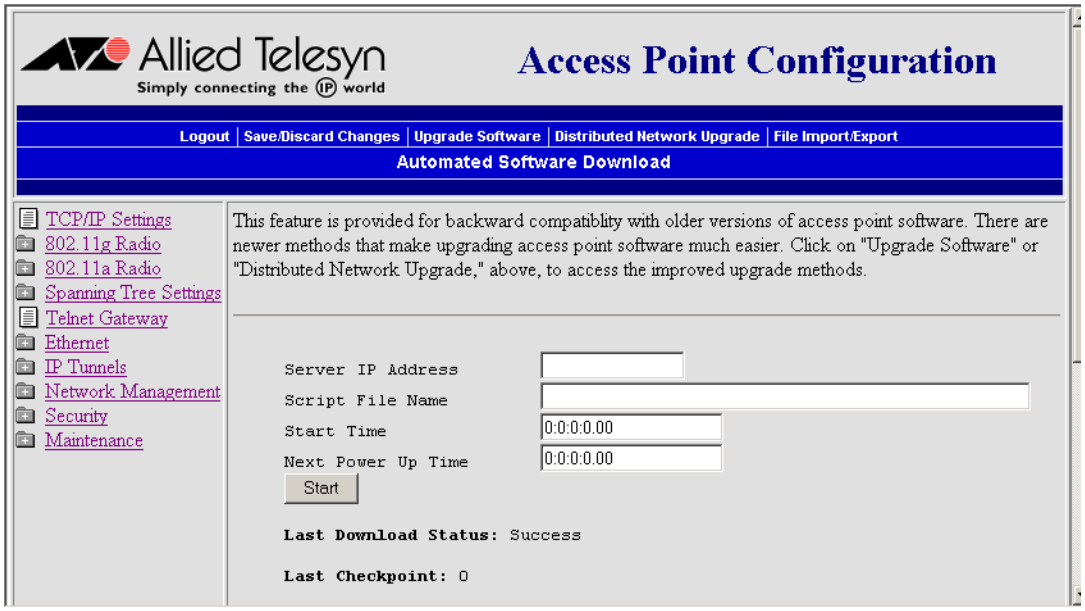
2. Click Stop Server to stop the TFTP server. Or click Start Server to start the TFTP server.

You can also use the TFTP SERVER START and STOP commands, described on page 282, to start and stop the TFTP server.

Automatically Upgrading Software

To automatically upgrade software (in a network with older access point software)

1. Click Upgrade software using automated software download. The Automated Software Download screen appears.



2. In the Server IP Address field, type the IP address of an active TFTP server from which the software download script file will be retrieved.
3. In the Script File Name field, type the name of a file on the TFTP server that contains the commands that define the download process.
4. In the Start Time field, enter the time in the format dd:hh:mm:ss (days:hours:minutes:seconds). When this timer expires, the access point performs a TFTP get to read the script file from the server and begins execution of the software download script.
5. In the Next Power Up Time field, enter the time in the format dd:hh:mm:ss (days:hours:minutes:seconds). When this timer expires, the access point will reboot, allowing the new firmware to take affect.
6. Click Start.

Appendix A
Specifications

This appendix contains AT-WA7500 and AT-WA7501 specifications for reference purposes only. Actual product performance and compliance with local telecommunications regulations may vary from country to country. Allied Telesyn only ships products that are type approved in the destination country.

AT-7500 Access Point

Table 80. AT-7500 Technical Specifications

Dimensions	H x L x W 4.6 cm x 25.0 cm x 15.9 cm (1.8 in x9.8 in x 6.3 in)
Weight	526 g (1.16 lb)
POE Electrical Rating	x 48V, 315 mA
Operating temperature	-20^{o}C to +55^{o}C (-4^{o}F to +131^{o}F)
Storage temperature	-40^{o}C to +70^{o}C (-40^{o}F to +158^{o}F)
Humidity (non-condensing)	10 to 90%
Architecture	Transparent bridge
Ethernet interfaces	10Base-T/100Base-TX (twisted-pair)
Ethernet compatibility	Ethernet frame types and Ethernet addressing
Ethernet data rate	10 Mbps/100 Mbps (Ethernet)
Radios supported	IEEE 802.11g, IEEE 802.11b, IEEE 802.11a
Media Access protocol	CSMA/CD
Filters (protocol)	IP, IPX, NetBEUI, DECNET, AppleTalk
Filters (others)	IP, ARP, Novell RIP, SAP, LSP
Serial port maximum data rate	115,200 bps
Management interfaces	Web browser-based manager, text-based menu system, serial port, Telnet, SNMP
SNMP agent	RFC 1213 (MIB-2), RFC 1398 (dot3), RFC 1493 (Bridge), 802.11, 802.1x
Regulatory Approvals	EN 550022/CISPR 22 Class A; FCC Part 15 & ICES-003 Class A; C tick Marked (AS 3548); CE Market, Compliant with RTT&E, EMC, LVD directives; (See separate radio approvals); UL Listed 1950 & IEC 60529-IP53; CSA Certified, C22.2 #950 & C22.3 #94-ENC 3.5; TUV Licensed, EN 60950 & EN 60529-IP53; NYCE Certified, NOM 19, plenum-rated

AT-7501 Access Point

Table 81. AT-7501 Technical Specifications

Dimensions	H x L x W 9.5 cm x 35.0 cm x 23.6 cm (3.8 in x 14.0 in x 5.8 in)
Weight	2.63 kg (5.8 lb)
AC electrical rating	Standard: ~100 to 240V, 1.0 to 0.5A, 50 to 60 Hz Heater (optional) ~100 to 120V, 1.0A, 50 to 60 Hz or ~200 to 240V, 0.5A, 50 to 60 Hz
POE Electrical Rating	x 48V, 315 mA
Operating temperature	Standard -25°C to +70°C (-13°F to +158°F) Heater (optional) AC only -30°C to +70°C (-22°F to +158°F) Heater/insulated bag (optional), AC only -30°C to +0°C (-22°F to +32°F)
Storage temperature	-40°C to +70°C (-40°F to +158°F)
Humidity (non-condensing)	10 to 90%
Industrial sealing	IP54 (NEMA 4)
Architecture	Transparent bridge
Ethernet interfaces	10Base-T/100Base-TX (twisted-pair)
Ethernet compatibility	Ethernet frame types and Ethernet addressing
Ethernet data rate	10 Mbps/100 Mbps (Ethernet) 100 Mbps (Fiber optic)
Fiber optic interface (optional)	MT-RJ
Radios supported	IEEE 802.11g, IEEE 802.11b, IEEE 802.11a
Media Access protocol	CSMA/CD
Filters (protocol)	IP, IPX, NetBEUI, DECNET, AppleTalk
Filters (others)	IP, ARP, Novell RIP, SAP, LSP

Table 81. AT-7501 Technical Specifications

Serial port maximum data rate	115,200 bps
Management interfaces	Web browser-based manager, text-based menu system, serial port, Telnet, SNMP
SNMP agent	RFC 1213 (MIB-2), RFC 1398 (dot3), RFC 1493 (Bridge), 802.11, 802.1x
Regulatory Approvals	EN 55022/CISPR 22 Class A; FCC Part 15 & ICES-003 Class A; C tick Marked (AS 3548); CE Market, Compliant with RTT&E, EMC, LVD directives; (See separate radio approvals); UL Listed 1950/C22.2 #950 IEC; 60529-IP53 and C22.2 #94-ENC 3.5; TUV Licensed, EN 60950 & EN 60539-IP53; NYCE Certified, NOM 19, plenum-rated

Radio Specifications

IEEE 802.11g

Table 82. IEEE 802.11g Radio Technical Specifications

Frequency band	2.4 to 2.5 GHz worldwide
Type	Direct sequence, spread spectrum
Modulation	Direct sequence, spread spectrum (CCK, DQPSK, DBPSK)
Power output	63 mW (18 dBm)
Basic data rate	11, 5.5, 2, and 1 Mbps
Extended data rate	54, 48, 36, 24, 18, 12, 9, and 6 Mbps
Channels	11 (North America), 13 (Europe), 4 (France), 14 (Japan). 1 (Israel)
Range (Maximum power output, 11 Mbps)[a]	160 m (525 ft) open environment 50 m (165 ft) semi-open environment 24 m (80 ft) in closed environment Unlimited range with roaming
Receiver sensitivity (11 Mbps)	-82 dBm
Security	IEEE 802.11 Wired Equivalent Privacy (WEP) standard, WEP 64, WEP 128, Wi-Fi Protected Access (WPA)

a. Lowering the power output level reduces the range.

IEEE 802.11b

Table 83. IEEE 802.11b Radio Technical Specifications

Frequency band	2.4 to 2.5 GHz worldwide
Type	Direct sequence, spread spectrum
Modulation	Direct sequence, spread spectrum (CCK, DQPSK, DBPSK)
Power output	32 mW (15 dBm)
Data rate	11 Mbps (High), 5.5 Mbps (Medium), 2 Mbps (Standard), 1 Mbps (Low) with automatic fallback for increased range

Table 83. IEEE 802.11b Radio Technical Specifications

Channels	11 (North America), 13 (Europe), 4 (France), 14 (Japan). 1 (Israel)
Range (11 Mbps)	160 m (525 ft) open environment 50 m (165 ft) semi-open environment 24 m (80 ft) in closed environment Unlimited range with roaming
Receiver sensitivity (11 Mbps)	-82 dBm
Security	IEEE 802.11 Wired Equivalent Privacy (WEP) standard, WEP 64, WEP 128, Wi-Fi Protected Access (WPA)

IEEE 802.11a

Table 84. IEEE 802.11a Radio Technical Specifications

Frequency band	Full range: 5.15 to 5.35 GHz (Indoor only) Mid range 5.25 to 5.35 GHz (Indoor and outdoor)
Type	Direct sequence, spread spectrum
Power output	40mW
Data rate	802.11 compliant mode: 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 12 Mbps, 6 Mbps with automatic fallback for increased range Turbo mode: 72 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 12 Mbps with automatic fallback for increased range
Channels	802.11 compliant mode (Full range): 8 (North America) 802.11 compliant mode (Mid range): 4 (North America) Turbo mode: 3 (North America)

Table 84. IEEE 802.11a Radio Technical Specifications

Range (depending on environment)	248 m (813.7 ft) 240 m (787.4 ft) 175 m (574.2 ft) 132 m (433.1 ft) 56 m (183.7 ft) 37 m (121.4 ft) 19 m (62.3 ft)	6 Mbps 12 Mbps 18 Mbps 24 Mbps 36 Mbps 48 Mbps 54 Mbps
Receiver sensitivity (54 Mbps)	-68 dBm	

Appendix B

Default Settings

This appendix provides factory defaults for reference purposes only.

The factory default settings for the access points are listed in this section. You can record the settings for your installation in each table for reference.

TCP/IP Settings Menu Defaults

Table 85. TCP/IP Settings Menu Defaults

Parameter Name	Range	Default	Your Site?
IP Address	4 nodes, 0 to 255 or DNS name	0.0.0.0	
IP Subnet Mask	4 nodes, 0 to 255	255.255.255.0	
IP Router (Gateway)	4 nodes, 0 to 255	0.0.0.0	
DNS Address 1	4 nodes, 0 to 255	0.0.0.0	
DNS Address 2	4 nodes, 0 to 255	0.0.0.0	
DNS Suffix 1	0 to 31 characters	(blank)	
DNS Suffix 2	0 to 31 characters	(blank)	
DHCP Mode	Always use DHCP, Use DHCP if IP Address is Zero, Disable DHCP, This AP is a DHCP Server	Use DHCP if IP Address is Zero	
DHCP Server Name	0 to 31 characters	(blank)	
DHCP User Class	DHCP user class identifier, as defined in RFC 2132	(blank)	
DHCP Vendor Class	DHCP vendor class identifier, as defined in RFC 2132	(blank)	

Table 85. TCP/IP Settings Menu Defaults

Parameter Name	Range	Default	Your Site?
DHCP for Access Point Network	Use Any Available DHCP Server, Only Use Access Point DHCP Server	Use Any Available DHCP Server	
Auto ARP Minutes	0 to 120	5	

DHCP Server Setup Menu Defaults

Table 86. DHCP Server Setup Menu Defaults

Parameter Name	Range	Default	Your Site?
Low Address	4 nodes, 0 to 255	10.10.10.100	
High Address	4 nodes, 0 to 255	10.10.10.199	
Lease Time	days:hours:minutes	0:00:20	
Permanently Save IP Address Mappings	Check/Clear	Clear	
IP Subnet Mask	4 nodes, 0 to 255	255.255.255.0	

IEEE 802.11g Radio Menu Defaults

Table 87. 802.11g Radio Menu Defaults

Parameter Name	Range	Default	Your Site?
Frequency	Channel 1 to 11, 2412 to 2462 MHz	Channel 03, 2422 MHz	
Node Type	Master, Station, Disabled	Master	
SSID (Network Name)	0 to 32 characters	atilan	
Member Limit	128 or 100	128 for Primary, 100 for Secondary	
Advanced Configuration			
Client Type/ Performance	11b/11g with range reliability (Not Wi-FI), 11b/11g with Wi-Fi compatible rates (Wi-Fi), 11g only for better throughput (Wi-Fi)	11b/11g with range reliability (Not Wi-FI)	
Power Output Level	Maximum, Medium, Low, Minimum	Maximum	
Enable Medium Reservation	Check/Clear	Clear	
Reservation Threshold (Appears if Enable Medium Reservation is enabled)	1 to 65535	500	
Fragmentation	256 to 2346	1600	

Table 87. 802.11g Radio Menu Defaults

Parameter Name	Range	Default	Your Site?
Antenna Control	Two Antennas/ One Antenna	One Antenna	
Mixed Mode Performance	Optimize Mixed (802.11b and 802.11g), Optimize for 802.11g clients, Optimize for 802.11b clients	Optimize Mixed (802.11b and 802.11g)	
Disallow Network Name of 'ANY'	Check/Clear	Clear	
DTIM Period	1 to 65535	1	
Inbound Filters (Primary Only)			
Allow IAPP	Check/Clear	Check	
Allow Wireless Transport Protocol (WTP)	Check/Clear	Check	
Allow UDP Plus (UDP/IP Port 5555)	Check/Clear	Check	
Allow DHCP	Check/Clear	Check	
Allow All Other Protocols	Check/Clear	Check	

IEEE 802.11b Radio Menu Defaults

Table 88. 802.11b Radio Menu Defaults

Parameter Name	Range	Default	Your Site?
Node Type	Master, Station, Disabled	Master	
SSID (Network Name)	0 to 32 characters	atilan	
Frequency	Channel 1 to 11, 2412 to 2462 MHz	Channel 03, 2422 MHz	
Advanced Configuration Parameters			
Data Rate	11, 5.5, 2, or 1 Mbps	11 Mbps (High)	
Allow Data Rate Fallback	Check/Clear	Check	
Basic Rate	11, 5.5, 2, or 1 Mbps	2 Mbps (Standard)	
Enable Medium Reservation	Check/Clear	Clear	
Reservation Threshold (Appears if Enable Medium Reservation is enabled)	1 to 65535	500	
Distance Between APs	Large, Medium, or Small	Large	
Enable Microwave Oven Robustness	Check/Clear	Clear	
Enable Load Balancing	Check/Clear	Clear	

Table 88. 802.11b Radio Menu Defaults

Parameter Name	Range	Default	Your Site?
Enable Medium Density Distribution	Check/Clear	Clear	
Data/Voice Settings	Data Traffic Only, Data and SpectraLink Traffic, SpectraLink Traffic Only	Data Traffic only	
Disallow Network Name of ‘ANY’	Check/Clear	Clear	
DTIM Period	1 to 65535	1	
Inbound Filters Parameters			
Allow IAPP	Check/Clear	Check	
Allow Wireless Transport Protocol (WTP)	Check/Clear	Check	
Allow SpectraLink Voice Protocol (SVP)	Check/Clear	Check	
Allow UDP Plus (UDP/IP Port 5555)	Check/Clear	Check	
Allow DHCP	Check/Clear	Check	
Allow All Other Protocols	Check/Clear	Check	

IEEE 802.11a Radio Menu Defaults

Table 89. 802.11a Radio Menu Defaults

Parameter Name	Range	Default	Your Site?
Frequency	Dynamic, 36, 40, 42, 44, 48, 50, 52, 56, 58, 60, 64	(full-range) Channel 36, 5180 MHz IEEE (mid-range) Channel 52, 5260 MHz IEEE	
Allow Wireless Access Points	On Primary On Secondary 1 On Secondary 2 On Secondary 3 Do not allow wireless access points	On Primary	
Node Type	Master, Station, Disabled	Master	
SSID (Network Name)	0 to 32 characters	atilan	
Advanced Configuration Parameters			
Power Output Level	Maximum, Medium, Low, Minimum	Maximum	
Data Rate	54, 48, 36, 24, 12, or 6 Mbps	54 Mbps (High)	
Allow Data Rate Fallback	Check/Clear	Check	
Basic Rate	24, 12, 6 Mbps	6 Mbps (Low)	
Reservation Threshold (2347 to Disable)	1 to 65535	2347	
Fragmentation Threshold	256 to 2346	2346	

Table 89. 802.11a Radio Menu Defaults

Parameter Name	Range	Default	Your Site?
Reservation Threshold (2347 to Disable)	1 to 65535	2347	
Fragmentation Threshold	256 to 2346	2346	
Disallow Network Name of ‘ANY’	Check/Clear	Clear	
Beacon Period	20 to 1000 TU	100	
DTIM Period	1 to 5	1	
Inbound Filters			
Allow IAPP	Check/Clear	Check	
Allow Wireless Transport Protocol (WTP)	Check/Clear	Check	
Allow UDP Plus (UDP/IP Port 5555)	Check/Clear	Check	
Allow DHCP	Check/Clear	Check	
Allow All Other Protocols	Check/Clear	Check	

Spanning Tree Settings Menu Defaults

Table 90. Spanning Tree Setting Menu Defaults

Parameter Name	Range	Default	Your Site?
AP Name	0 to 16 characters	(access point serial number)	
LAN ID (Domain)	0 to 254	0	
Root Priority	0 to 7	1	
Enable Ethernet Bridging	Check/Clear	Check	
Enable GVRP for VLAN	Check/Clear	Clear	
Rightmost LED Behavior	Ready-to-Work Indicator/ Spanning Tree Root Indicator	Ready-to-Work	
Enable Ethernet Bridging	Check/Clear	Check	
Secondary LAN Bridge Priority	0 to 7	0	
Secondary LAN Flooding	Enabled, Multicast, Unicast, Disabled	Disabled	

Global Flooding Menu Defaults

Table 91. Global Flooding Menu Defaults

Parameter Name	Range	Default	Your Site?
Multicast Flooding	Universal, Hierarchical, Disabled	Hierarchical	
Multicast Outbound to Secondary LANs	Enabled globally/Set locally	Set locally	
Allow Multicast Outbound to Terminals	Check/Clear	Check	
Unicast Flooding	Universal, Hierarchical, Disabled	Disabled	
If Unicast Flooding is Universal or Hierarchical			
Unicast Outbound to Secondary LANs	Enabled globally/Set locally	Set locally	
Allow Unicast Outbound to Terminals	Check/Clear	Check	
Enable ARP Flooding	Check/Clear	Check	

Global RF Parameters Menu Defaults

Table 92. Global RF Parameters Menu Defaults

Parameter Name	Range	Default	Your Site?
Perform RFC1042/DIX Conversion	Check/Clear	Check	
S-UHF Rfp Threshold			
Set Globally	Enabled/ Disabled	Disabled	
Value	0 to 250 bytes	70 bytes	
S-UHF Frag Size			
Set Globally	Enabled/ Disabled	Disabled	
Value	50 to 250 bytes	250 bytes	
902 MHz Frag Size			
Set Globally	Enabled/ Disabled	Disabled	
Value	50 to 250 bytes	250 bytes	
S-UHF/902 MHz Awake Time			
Set Globally	Enabled/ Disabled	Disabled	
Value	0 to 250 tenths of a second	10 (902 MHz) 20 (S-UHF)	
RFC1042 Types to Pass Through			
1	Two sets of hexadecimal pairs 00 through FF.	80 F3	
2	Two sets of hexadecimal pairs 00 through FF.	81 37	

Table 92. Global RF Parameters Menu Defaults

Parameter Name	Range	Default	Your Site?
3 through 20	Two sets of hexadecimal pairs 00 through FF.	00 00	

Telnet Gateway Configuration Menu Defaults

Table 93. Telnet Gateway Configuration Menu Defaults

Parameter Name	Range	Default	Your Site?
Host Name	IP address or DNS name	(blank)	
Host Port	23	23	
Term Port	Off, 23,5000, 5001, 5002, 5003, 5004, 5005, 5006, 5007, 5008, 5008	Off	
Idle Time	1 to 255	0 (disabled)	
Lost Time	1 to 255	0 (disabled)	

Ethernet Configuration Menu Defaults

Table 94. Ethernet Configuration Menu Defaults

Parameter Name	Range	Default	Your Site?
Port Type	10/100 Mb Twisted-Pair 100 Mb Fiber Optic	10/100 Mb Twisted-Pair	
Link Speed	Auto Select, 100 Mbps Full-Duplex, 100 Mbps Half-Duplex, 10 Mbps Full-Duplex, 10 Mbps Half-Duplex	Auto Select	
Enable Link Status Check	Check/Clear	Clear	
Address Table			
1 through 20	Six sets of hexadecimal pairs 00 through FF.	00 00 00 00 00 00	
Frame Type Filters			
Allow/Pass	Check/Clear	Check	
Scope	Unlisted/All	Unlisted	
Predefined Subtype Filters			
Allow/Pass	Check/Clear	Check	

Ethernet Advanced Filters Menu Defaults

Table 95. Ethernet Advanced Filters Menu Defaults

Parameter Name	Range	Default	Your Site?
Customizable Subtype Filters			
Allow/Pass	Check/Clear	Check	
SubType	DIX-IP-TCP-Port, DIX-IP-UDP-Port, DIX-IP-Protocol, DIX-IPX-Socket, DIX-EtherType, SNAP-IP-TCP-Port, SNAP -IP-UDP-Port, SNAP -IP-Protocol, SNAP -IPX-Socket, SNAP -EtherType, 802.3-IPX-Socket, 802.2 -IPX-Socket, 802.2-SAP	DIX-IP-TCP-Port	
Value	Two sets of hexadecimal pairs 00 through FF.	00 00	
Filter Values			
Value ID		0	
Value		(blank)	
Filter Expressions			
ExprSeq		0	
Offset		0	
Mask		(blank)	
Op	EQ, NE, GT, LE	EQ	
Value ID		0	
Action	And, Pass, Drop	And	

IP Tunnels Menu Defaults

Table 96. IP Tunnels Menu Defaults

Parameter Name	Range	Default	Your Site?
Mode	Listen, Originate If Root, Disabled	Listen	
Enable IGMP (Appears if Mode is Listen)	Check/Clear	Clear	
Multicast Address (Appears if Enable IGMP is checked)	4 nodes, 0 to 255	224.0.1.65	
Allow IP Multicast (Appears if Mode is Originate if Root)	Check/Clear	Clear	
IP Addresses (1-8) (Appears if Mode is Originate if Root)	4 nodes, 0 to 255 or DNS name up to 31 characters	(blank)	

Tunnels Filter Menu Defaults

Table 97. Tunnel Filters Menu Defaults

Parameter Name	Range	Default	Your Site?
Frame Type Filters			
Allow/Pass	Check/Clear	Clear	
Scope	Unlisted/All	Unlisted	
Predefined Subtype Filters			
Allow/Pass	Check/Clear	Clear (except Check for NNL)	
Customizable Subtype Filters			
Allow/Pass	Check/Clear	Clear	

Table 97. Tunnel Filters Menu Defaults

Parameter Name	Range	Default	Your Site?
SubType	DIX-IP-TCP-Port, DIX-IP-UDP-Port, DIX-IP-Protocol, DIX-IPX-Socket, DIX-EtherType, SNAP-IP-TCP-Port, SNAP -IP-UDP-Port, SNAP -IP-Protocol, SNAP -IPX-Socket, SNAP -EtherType, 802.3-IPX-Socket, 802.2 -IPX-Socket, 802.2-SAP	DIX-IP-TCP-Port	
Value	Two sets of hexadecimal pairs 00 through FF.	00 00	

Network Management Menu Defaults

Table 98. Network Management Menu Defaults

Parameter Name	Range	Default	Your Site?
SNMP Read Community	1 to 15 characters	public	
SNMP Write Community	1 to 15 characters	CR52401	
SNMP Secret Community	1 to 15 characters	Secret	
Avalanche Agent Name	IP address or DNS name	(blank)	

Instant On Menu Defaults

Table 99. Instant On Menu Defaults

Parameter Name	Range	Default	Your Site?
Enable Instant On Server	Check/Clear	Clear	
Enable Secure Credential Creation (Appears if Enable Instant On Server is enabled)	Check/Clear	Clear	

Security Menu Defaults

Table 100. Security Menu Defaults

Parameter Name	Range	Default	Your Site?
Browser Access	Secure-Only (Port 443), Enabled (Port 80/443), Disabled	Enabled (Port 80/443)	
Allow Telnet Access (Port 23)	Check/Clear	Check	
Allow SNMP Access (Port 161/162)	Check/Clear	Check	
Allow TFTP Access (Read-Only)	Check/Clear	Check	
Allow ICMP Configuration	Check/Clear	Check	
Allow Avalanche Access	Check/Clear	Check	

Passwords Menu Defaults

Table 101. Password Menu Defaults

Parameter Name	Range	Default	Your Site?
Use RADIUS for Login Authorization	Check/Clear	Clear	
User Name	1 to 32 characters (Not case sensitive)	atilan	

Table 101. Password Menu Defaults

Parameter Name	Range	Default	Your Site?
Password	1 to 32 characters (Not case sensitive)	atilan	
Read Only Password	1 to 32 characters (Not case sensitive)	(blank)	
Allow Service Password	Check/Clear	Check	

IEEE 802.11 (g, b or a) Radio Security Menu Defaults

Table 102. IEEE 802.11g/b/a Radio Security Menu Defaults

Parameter Name	Range	Default	Your Site?
Enable ACL Client Authorization	Check/Clear	Clear	
Enable Alternative Method ACL	Check/Clear	Clear	
ACL RADIUS Client Password (Appears if Enable ACL Client Authorization is enabled)	1 to 32 characters Must match the password configured in the external RADIUS server)	wireless	
VLAN	1-4094	1 (Disabled)	
Security Level	None, Static WEP, Dynamic WEP/802.1x, WPA/PSK, WPA + 802.1x	None	

Table 102. IEEE 802.11g/b/a Radio Security Menu Defaults

Parameter Name	Range	Default	Your Site?
If Security Level is Static WEP			
WEP Transmit Key	1, 2, 3, or 4	1	
WEP Key 1 to 4	5 ASCII characters (or hex pairs) to 16 ACSII characters (or hex pairs)	80211	
If Security Level is Dynamic WEP/802.1x			
Key Rotation Period	Any number	5	
If Security Level is WPA/PSK			
Multicast Encryption Type	TKIP	TKIP	
Pre-share Key	256 (32 byte) hexadecimal value or an ASCII pass-phrase	(blank)	
Key Rotation Period	Any number	5	
If Security Level is WPA + 802.1x			
Multicast Encryption Type	WEP, TKIP	TKIP	
Key Rotation Period	Any number	5	

RADIUS Server List Menu Defaults

Table 103. RADIUS Server List Menu Defaults

Parameter Name	Range	Default	Your Site?
IP Address/ DNS name	4 nodes, 0 to 255 or DNS name	0.0.0.0	
Secret Key	16 to 32 bytes	(factory default)	
Port	1-65535 Recommended range is 49152-65535	1812	
802.1x	Check/Clear	Clear except Servers 5 and 6	
ACL	Check/Clear	Clear except Servers 3 and 4	
Login	Check/Clear	Clear except Servers 1 and 2	

Spanning Tree Security Menu Defaults

Table 104. Spanning Tree Security Menu Defaults

Parameter Name	Range	Default	Your Site?
Secure IAPP	Check/Clear	Clear	
If 802.1x security or Secure IAPP is enabled			
IAPP Secret Key	16 to 32 bytes	(factory default)	
Allow SWAP	Check/Clear	Check	
Allow TLS	Check/Clear	Clear	
Allow TTLS	Check/Clear	Check	
Preferred Protocol	SWAP/TLS/ TTLS	TTLS	
User Name	1 to 31 characters	anonymous	

Table 104. Spanning Tree Security Menu Defaults

Parameter Name	Range	Default	Your Site?
Password	1 to 31 characters	anonymous	
Verify CA Certificate	Check/Clear	Clear	

Embedded Authentication Server Menu Defaults

Table 105. Embedded Authentication Server Menu Defaults

Parameter Name	Range	Default	Your Site?
Enable Server	Check/Clear	Clear	
If Enable Server is enabled			
Default Secret Key	16 to 32 bytes	(factory default)	
UDP Port	49152-65535	1812	
Authorization Time	hh:dd:mm	0:01:00	
Enable PEAP Fast Reconnect	Check/Clear	Check	

Appendix C
Glossary

ARP (Address Resolution Protocol) cache

A table that stores IP addresses and their corresponding MAC addresses. The access point maintains an ARP cache and can act as an ARP server.

BFSK (Binary Frequency Shift Key)

A broadcasting method that lengthens the range but halves the throughput as compared to the QFSK method. In access points using an OpenAir radio, the radio can be configured so that it automatically switches to this method when the RF protocol determines that throughput is degrading due to range. The transmit mode parameter determines if BFSK will be used. The default setting for transmit mode is AUTO, which allows this automatic switching to occur.

broadcast

A type of transmission in which a message sent from the host is received by many devices on the system.

data link tunneling

An access point feature that encapsulates the data into an OWL data frame. This frame is then forwarded via the Ethernet port to the next access point on the path and so on until the frame reaches the root access point or designated bridge. The root access point or designated bridge unencapsulates the frame and forwards it to the host. When the root access point or designated bridge receives data on the Ethernet network for an end device, it reverses this process.

You should only use data link tunneling if you have Ethernet switches that do not support the IEEE 802.1d requirements for backward learning or if you are using IP tunnels to provide mobility of other routable protocols.

To enable data link tunneling, disable Ethernet bridging.

designated bridge

Also called a secondary LAN bridge. An access point that is assigned the role of bridging frames destined for or received from a secondary LAN. A designated bridge connects a secondary LAN with the primary LAN. In the access point, the secondary LAN bridge priority parameter determines if the access point is a candidate to become the designated bridge.

DHCP (Dynamic Host Configuration Protocol)

An Internet standard stack protocol that allows dynamic distribution of IP address and other configuration information to IP hosts on a network. Implementation of the DHCP client in Allied Telesyn network devices simplifies installation because the devices automatically receive IP addresses from a DHCP server on the network.

directional antenna

An antenna (often called a yagi) that transmits and receives RF signals more in one direction than others. This radiation pattern is similar to the light that a flashlight produces. These antennas have a narrower beam width, which limits coverage on the sides of the antennas. Directional antennas have much higher gain than omni antennas and work best for covering large narrow areas or on point-to-point bridges.

distribution LAN

Any Ethernet LAN attached to access points that are bridging between the Ethernet LAN and the radio network. At any given time, only one access point in a distribution LAN provides access to the Ethernet LAN for a given node in the domain.

DIX

A standardized Ethernet frame format developed by Digital Equipment Corporation, Intel Corporation, and Xerox. Another frame format is 802.3.

EAP (Extensible Authentication Protocol)

Used in 802.1x-enabled networks. A standard mechanism for support of different authentication methods. EAP authentication types provide devices with secure connections to the network as well as protect credentials and data privacy. See also "TLS" and "TTLS."

Ethernet bridging

When an access point receives wireless traffic and the destination address is known, it forwards frames to the port with the shortest path to the destination address. When the access point has not learned the direction of the shortest path for the destination address, it forwards frames based on flooding settings to try to locate the destination address.

flooding

A frame is flooded when the destination location is unknown. The destination location of a multicast frame is never known. Unicast and multicast flooding parameters determine how a flooded frame is forwarded.

hello period

A time increment (usually 1, 2, or 3 seconds) that determines how often the access point sends out a type of multicast frame so that it can dynamically discover and test connections to other devices in the network. Once this information is learned, the access point and routers can exchange routing information.

home IP subnet

Also called the root IP subnet and primary LAN. The IP subnet that contains the root access point. If wireless end devices need to roam between IP subnets, each end device needs to have an IP address from the home IP subnet.

IAPP (Inter Access Point Protocol)

Access points use this protocol to communicate with each other. For example, when a wireless end device roams to a new access point, the new access point informs the old access points via the root access point that any traffic for the end device needs to be routed to the new access point.

This protocol also allows 802.1x-ready devices to roam seamlessly through the network without having to reauthenticate after each roam. IAPP distributes security credentials throughout the network. When an end device roams from one access point to another, its credentials are also transferred.

Secure IAPP prevents unauthorized Allied Telesyn access products from joining the spanning tree and it encrypts IAPP frames. If you enable secure IAPP, access points will use SWAP to create secure wireless hops when communicating with each other.

IGMP (Internet Group Management Protocol)

A standard protocol that lets you originate multiple IP tunnels using one IP multicast address. IGMP allows IP multicast frames to be routed to remote IP subnets that have hosts participating in the multicast group. By enabling IGMP, access points can act as IP hosts and participate in an IP multicast group.

inbound frames

Frames moving toward the primary LAN.

IP router

A software and hardware connection between two or more subnetworks that permits traffic to be routed from one network to another on the basis of the intended destinations.

IP subnet

A single member of the collection of hardware networks that comprise an IP network. Host addresses on a given subnet share an IP network number with hosts on all other subnets of the IP network. The local address is divided into subnet-number and host-number fields to indicate which subnet a host is on.

IP tunneling

IP tunneling is used on networks with routers. IP tunneling allows wireless end devices to roam across IP subnet boundaries without losing connection. IP tunneling encapsulates standard IP frames with Generic Routing Encapsulation (GRE) and forwards the frames from the root access point on a home IP subnet to another access point on a remote IP subnet. IP tunneling is done through the access points' logical IP ports.

MAC address

There are two types of MAC addresses: unicast and broadcast. Unicast specifies a single Ethernet interface, while multicast specifies a group of Ethernet addresses. Broadcast is a variation of multicast in which a multicast is received by all interfaces.

MIB (Management Information Base)

This repository stores network traffic information that SNMP management programs collect. Your network administrator can use management software interacting with the MIB to obtain information about network

activity. The MIB for the access point is available from the Allied Telesyn web site at www.alliedtelesyn.com.

multicast address

A form of broadcast address through which copies of the frame are delivered to a subset of all possible destinations that have a common multicast address.

NAT (Network Address Translation)

A mechanism for reducing the need for different IP addresses. NAT allows an organization with IP addresses that are not unique to connect to the network by translating those addresses into routable address space. The access point can act as a DHCP/NAT server.

non-bridging secondary LAN

A secondary LAN that does not have a designated bridge. A non-bridging secondary LAN is used to interconnect access points without using wireless hops.

omni antenna

An antenna that transmits and receives RF signals in all directions equally on a horizontal plane. This radiation pattern is similar to a doughnut with the antenna being in the center of the doughnut hole. These antennas provide the widest coverage and are most commonly used inside buildings.

outbound frames

Frames moving away from the primary LAN.

peer-to-peer network

A type of LAN whose workstations are capable of being both clients and servers.

point-to-multipoint bridge

See also wireless bridge. A bridge that connects two wired networks with similar architectures. Two access points can be used to provide a point-to-multipoint bridge between two buildings so that wired and wireless devices in each building can communicate with devices in the other building. A point-to-multipoint bridge has two radios, which allows wireless end devices to communicate with it.

point-to-point bridge

See also wireless bridge. A bridge that connects two wired networks with similar architectures. Two access points can be used to provide a point-to-point bridge between two buildings so that wired and wireless devices in each building can communicate with devices in the other building.

power bridge

A power bridge combines power and data onto an Ethernet cable that is connected to the access point with the power over Ethernet option.

primary bridging

Ethernet bridging on a root port. An access point uses primary bridging to bridge frames to and from the Ethernet network on its root port. Note that primary bridging is not the same as bridging to the primary LAN.

primary LAN

Also called the home IP subnet and root IP subnet. The IP subnet that contains the root access point. The primary LAN is typically the LAN on which the servers are located.

QFSK (Quad Frequency Shift Key)

A broadcasting method that shortens the range but doubles the throughput as compared to the BFSK method. In access points using a 2.4 GHz OpenAir radio, the radio can automatically switch between QFSK and BFSK as needed if the transmit mode is set to AUTO.

remote IP subnet

An IP subnet that is separated from the primary IP subnet (primary LAN) by a router. Remote IP subnets communicate with the primary LAN through IP tunnels. A remote IP subnet is a type of secondary LAN.

root access point

The access point with the highest root priority becomes the root of the network spanning tree. If the root becomes inactive, the remaining root candidates negotiate to determine which access point becomes the new root. The root can be used to set system-wide flooding and RF parameters. The root is also the only node in the network that can originate IP tunnels.

root port

The access point port that provides the inbound connection to the spanning tree. The root port provides a link to a parent access point. Note that a root access point does not have a root port.

root IP subnet

Also called the home IP subnet and primary LAN. The IP subnet that contains the root access point. If wireless end devices need to roam between IP subnets, each end device needs to have an IP address from the root IP subnet.

secondary bridging

Ethernet bridging on a non-root port. An access point that is the designated bridge for a secondary LAN uses secondary bridging to bridge frames to and from the secondary LAN on a non-root port.

secondary LAN

Any LAN that is reached by routing traffic through an access point. Wireless end devices that are communicating through a WAP comprise a secondary LAN. A remote IP subnet is a type of secondary LAN.

service set

A logical (not physical) radio. You can create up to four service sets for each physical 802.11g and 802.11a radio in an access point. Each service set shares the same physical radio configuration (including the parameters set for Advanced Configuration and Inbound Filters). Each service set has a unique SSID (network name), and you may customize its security configuration and member limit. Multiple service sets are used primarily to allow one radio to support multiple VLANs.

SNAP

A protocol extension typically used by AppleTalk networks.

SNMP (Simple Network Management Protocol)

SNMP is a popular network management protocol in the TCP/IP and SPX/IPX protocol suite. SNMP allows TCP/IP and SPX/IPX sites to exchange configuration and status information. It uses management programs called “agents” to monitor network traffic. SNMP stores the information it collects in the Management Information Base (MIB). Your network administrator can use management software, such as MobileLAN manager, interacting

with the MIB to obtain information about network activity.

spanning tree

A form of network organization in which each device on the network has only one path to the root. The access points automatically configure into a self-organized network that provides efficient, loop-free forwarding of frames through the network.

splitter

A splitter converts 48V input power to 5V or 3.3V output power. If you want to use power over Ethernet, you plug the access point into the splitter and then you plug the splitter into a power bridge.

The AT-WA7500 and AT-WA7501 do not use a splitter.

SWAP (Secure Wireless Authentication Protocol)

This protocol creates secure wireless hops if you enable secure IAPP. It forces access points to authenticate each other using an EAP-MD5 challenge.

Telnet Gateway

A software feature in Release 2.1 that allows the access point to keep telnet sessions alive even when the wireless client is idle or disconnected for any reason (because the client has roamed out of range, been powered off, lost battery power, etc.).

TLS (Transport Layer Security)

An EAP authentication type that not only requires a certificate on the authentication server, but also one on the end device. There is both server and client side authentication before the end device can communicate with the network.

TTLS (Tunneled Transport Layer Security)

An EAP authentication type that only requires a certificate on the authentication server. End devices have a user name and password that proves that they are authorized to communicate with the network.

triangular routing

The routing logic used for a mobile IP end device that has roamed to a foreign network. Frames destined for a mobile end device are always sent

to the home subnet of the end device. If the end device has roamed to another subnet, the frame must be forwarded to the remote subnet where the end device currently resides.

unicast address

A unique Ethernet address assigned to a single device on the network.

VLAN (virtual LAN)

A network of wireless end devices that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a local area network. You can group all wireless users on a particular VLAN in order to manage the IP address space differently. Or you can use VLANs to separate secure and non-secure traffic.

WAP (Wireless Access Point)

Also called a repeater. This access point does not have any connections on its Ethernet port. It forwards data between the access point and the secondary LAN.

WEP (Wired Equivalent Privacy) encryption

A feature that can be enabled in the IEEE 802.11b or 802.11a radio that allows data encryption for wireless communications.

wireless bridge

Also called a point-to-point bridge. A wireless link that connects two wired Ethernet segments. Two access points can be used to provide a wireless bridge between two buildings, so that wired and wireless devices in each building can communicate with devices in the other building.

wireless hop

A wireless link that occurs when data from a wireless end device moves from one access point to another access point through the radio ports. Using Allied Telesyn access products, Allied Telesyn recommends that your data does not travel through more than three wireless hops.

Secure wireless hops are created when secure IAPP is enabled. Access points use SWAP to authenticate each other.

WPA (Wi-Fi Protected Access)

A feature that can be implemented in the 802.11g, 802.11b, and 802.11a radios for security in a wireless network. WPA is a strongly enhanced, interoperable Wi-Fi security protocol that addresses many of the vulnerabilities of WEP. It provides stronger RC4 encryption over standard WEP with TKIP.